# **Elastic Graph Neural Networks**

Xiaorui Liu

Joint work with Wei Jin (co-first author), Yao Ma, Yaxin Li, Hua Liu, Yiqi Wang, Ming Yan & Jiliang Tang

Michigan State University

ICML 2021, July 21st

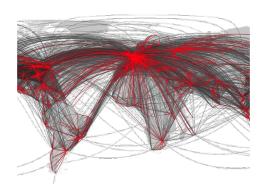




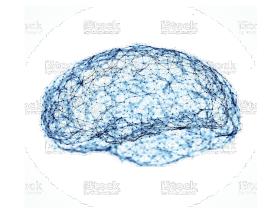
# Data as Graphs



Social Graphs



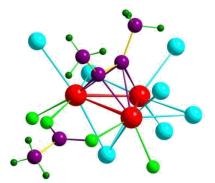
Transportation Graphs



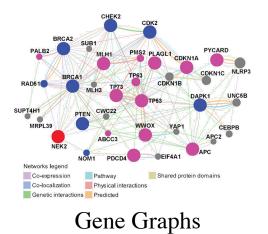
Brain Graphs



Web Graphs

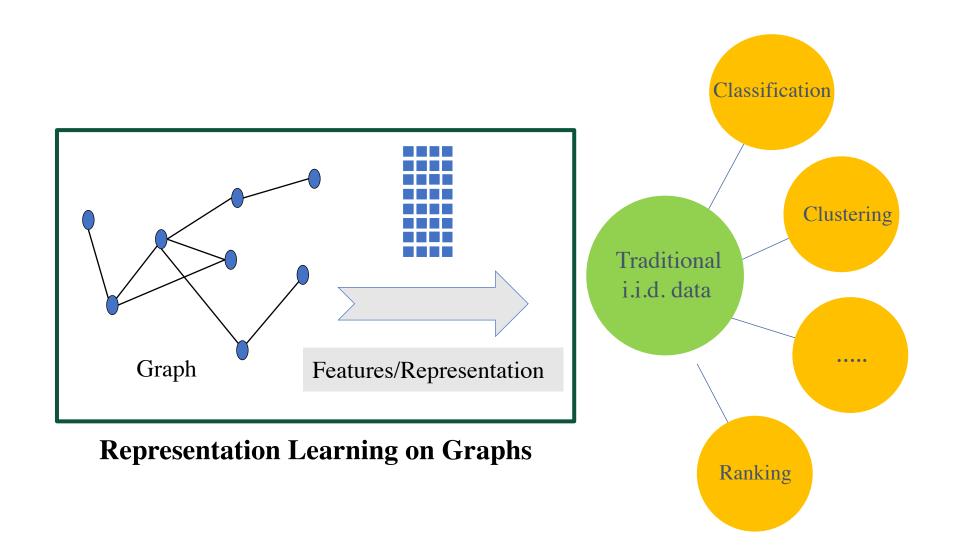


Molecular Graphs





# Machine Learning on Graphs

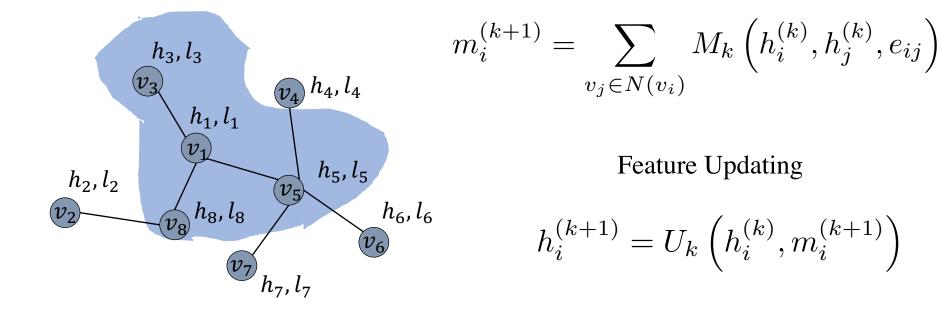






## Graph Neural Networks

Message Passing

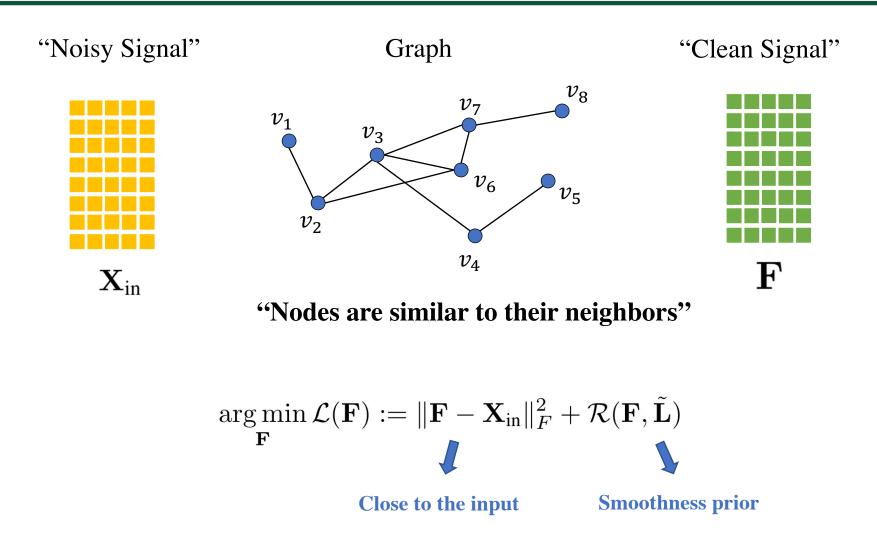


Neural Message Passing for Quantum Chemistry, Justin Gilmer et al, ICML 2017

#### Data Science and Engineering Lab

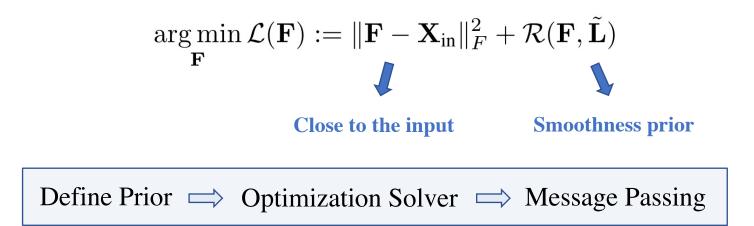


# A Unified View on Message Passing



A unified view on graph neural networks as graph signal denoising, Yao Ma, Xiaorui Liu et al, 2020

# A Unified View on Message Passing



**Example** 
$$\mathcal{R}(\mathbf{F}, \tilde{\mathbf{L}}) = \lambda \operatorname{tr}(\mathbf{F}^{\top} \tilde{\mathbf{L}} \mathbf{F}) = \lambda \sum_{(v_i, v_j) \in \mathcal{E}} \|\frac{\mathbf{F}_i}{\sqrt{d_i + 1}} - \frac{\mathbf{F}_j}{\sqrt{d_j + 1}}\|_2^2$$

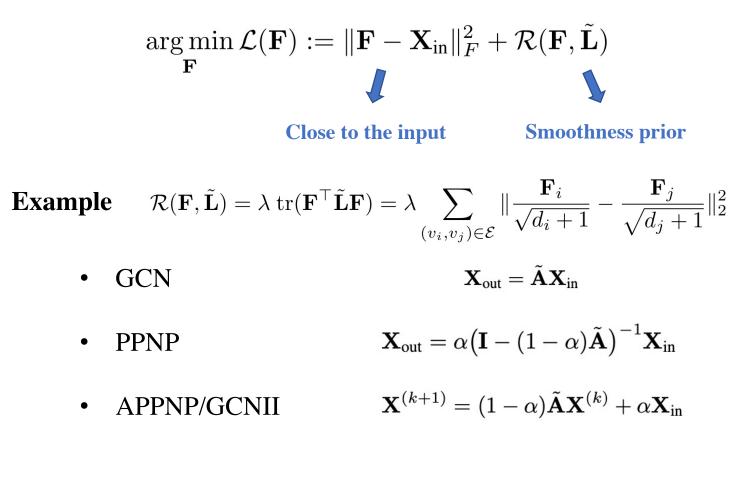
• GCN 
$$\mathbf{X}_{out} = \tilde{\mathbf{A}} \mathbf{X}_{in}$$

- PPNP  $\mathbf{X}_{out} = \alpha \left( \mathbf{I} (1 \alpha) \tilde{\mathbf{A}} \right)^{-1} \mathbf{X}_{in}$
- APPNP/GCNII  $\mathbf{X}^{(k+1)} = (1-\alpha)\tilde{\mathbf{A}}\mathbf{X}^{(k)} + \alpha\mathbf{X}_{in}$

A unified view on graph neural networks as graph signal denoising, Yao Ma, Xiaorui Liu et al, 2020



## **Global Smoothness**

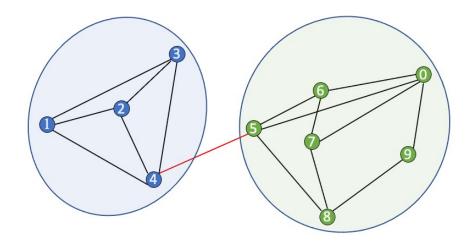


These MP schemes enforce global smoothness shared across the whole graph



Can we enhance local smoothness adaptively across different region over the graph?

Noise graph structure

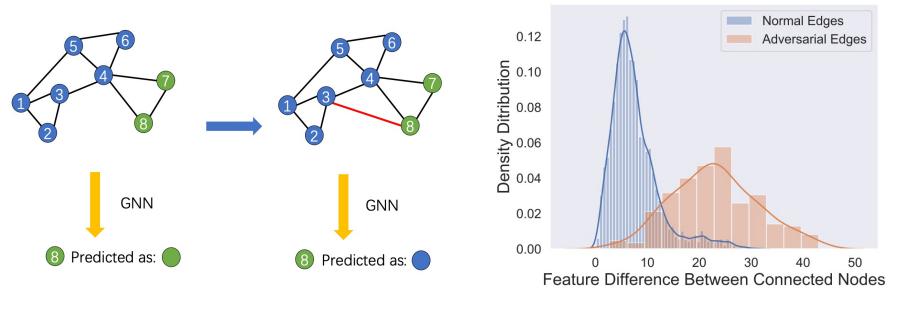






# Local Smoothness

#### Adversarial graph attack



Graph attack

Feature smoothness

Graph Structure Learning for Robust Graph Neural Networks,

Wei Jin, Yao Ma, Xiaorui Liu, et al, KDD 2020.



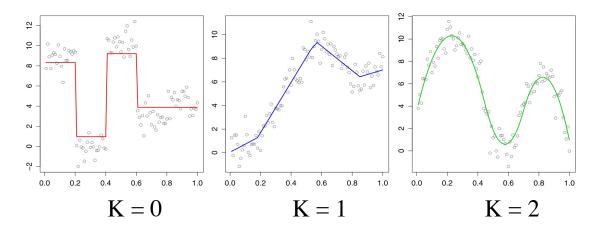
# **Trend Filtering**

**Nonparametric regression** (univariate)

$$\hat{\beta} = \underset{\beta \in \mathbb{R}^{n}}{\operatorname{argmin}} \frac{1}{2} \| y - \beta \|_{2}^{2} + \frac{n^{k}}{k!} \cdot \lambda \| D^{(k+1)} \beta \|_{1} \qquad D^{(1)} = \begin{bmatrix} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix} \in \mathbb{R}^{(n-1) \times n}$$

$$D^{(k+1)} = D^{(1)} \cdot D^{(k)}$$

#### Adapt to the local level of smoothness



*L*<sub>1</sub> Trend filtering, S.-J. Kim et al, SIAM Review, 2009

Adaptive piecewise polynomial estimation via trend filtering, Ryan Tibshirani, Annals of Statistics, 2014



# Graph Trend Filtering

GTF

$$\underset{\mathbf{f}\in\mathbb{R}^n}{\operatorname{arg\,min}} = \frac{1}{2} \|\mathbf{f} - \mathbf{x}\|_2^2 + \lambda \|\Delta^{(k+1)}\mathbf{f}\|_1$$

**Incident matrix** 

$$\Delta_{\ell} = (0, \dots, \underbrace{-1}_{i}, \dots, \underbrace{1}_{j}, \dots, 0)$$

$$\|\Delta^{(1)}\mathbf{f}\|_1 = \sum_{(v_i, v_j) \in \mathcal{E}} |\mathbf{f}_i - \mathbf{f}_j|$$

$$\Delta^{(k+1)} = \begin{cases} \Delta^{\top} \Delta^{(k)} = \mathbf{L}^{\frac{k+1}{2}} \in \mathbb{R}^{n \times n} & \text{for odd } \mathbf{k} \\ \Delta \Delta^{(k)} = \Delta \mathbf{L}^{\frac{k}{2}} \in \mathbb{R}^{m \times n} & \text{for even } \mathbf{k} \end{cases}$$

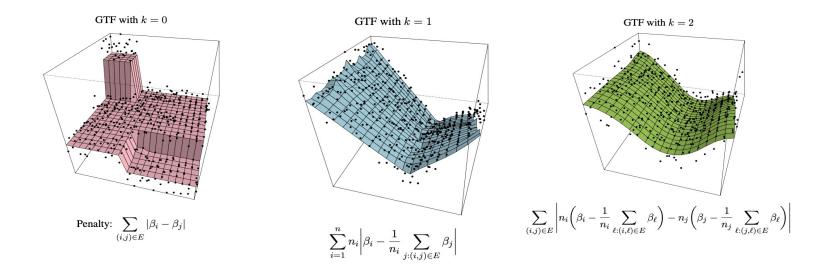
Trend filtering on graphs, Yu-Xiang Wang et al, JMLR 2016



# Graph Trend Filtering

$$rgmin_{\mathbf{f}\in\mathbb{R}^n} = rac{1}{2}\|\mathbf{f}-\mathbf{x}\|_2^2 + \lambda\|\Delta^{(k+1)}\mathbf{f}\|_1$$

#### Local smoothness adaptivity: piecewise behavior



Trend filtering on graphs, Yu-Xiang Wang et al, JMLR 2016





## Elastic Graph Signal Estimator

$$\arg \min_{\mathbf{F}} \mathcal{L}(\mathbf{F}) := \|\mathbf{F} - \mathbf{X}_{in}\|_{F}^{2} + \mathcal{R}(\mathbf{F}, \tilde{\mathbf{L}})$$
Close to the input Smoothness prior
$$\mathcal{R}(\mathbf{F}, \tilde{\mathbf{L}}) = \lambda_{1} \|\tilde{\Delta}\mathbf{F}\|_{1} + \frac{\lambda_{2}}{2} \operatorname{tr}(\mathbf{F}^{\top}\tilde{\mathbf{L}}\mathbf{F}) \qquad \tilde{\Delta} = \Delta \hat{\mathbf{D}}^{-\frac{1}{2}}$$

$$\|\tilde{\Delta}\mathbf{F}\|_{1} = \sum_{(v_{i}, v_{j}) \in \mathcal{E}} \left\|\frac{\mathbf{F}_{i}}{\sqrt{d_{i}+1}} - \frac{\mathbf{F}_{j}}{\sqrt{d_{j}+1}}\right\|_{1} \qquad \operatorname{tr}(\mathbf{F}^{\top}\tilde{\mathbf{L}}\mathbf{F}) = \sum_{(v_{i}, v_{j}) \in \mathcal{E}} \left\|\frac{\mathbf{F}_{i}}{\sqrt{d_{i}+1}} - \frac{\mathbf{F}_{j}}{\sqrt{d_{j}+1}}\right\|_{2}^{2}$$
Coupling multi-dimensionality
$$\mathcal{R}(\mathbf{F}, \tilde{\mathbf{L}}) = \lambda_{1} \|\tilde{\Delta}\mathbf{F}\|_{21} + \frac{\lambda_{2}}{2} \operatorname{tr}(\mathbf{F}^{\top}\tilde{\mathbf{L}}\mathbf{F})$$

$$\|\tilde{\Delta}\mathbf{F}\|_{21} = \sum_{(v_{i}, v_{j}) \in \mathcal{E}} \left\|\frac{\mathbf{F}_{i}}{\sqrt{d_{i}+1}} - \frac{\mathbf{F}_{j}}{\sqrt{d_{j}+1}}\right\|_{2} \qquad \operatorname{tr}(\mathbf{F}^{\top}\tilde{\mathbf{L}}\mathbf{F}) = \sum_{(v_{i}, v_{j}) \in \mathcal{E}} \left\|\frac{\mathbf{F}_{i}}{\sqrt{d_{i}+1}} - \frac{\mathbf{F}_{j}}{\sqrt{d_{j}+1}}\right\|_{2}^{2}$$

~ .



### Elastic Graph Signal Estimator

$$\begin{aligned} \mathbf{Option I} \qquad & \underset{\mathbf{F} \in \mathbb{R}^{n \times d}}{\operatorname{arg min}} \underbrace{\lambda_1 \| \tilde{\Delta} \mathbf{F} \|_1}_{g_1(\tilde{\Delta} \mathbf{F})} + \underbrace{\frac{\lambda_2}{2} \operatorname{tr}(\mathbf{F}^\top \tilde{\mathbf{L}} \mathbf{F}) + \frac{1}{2} \| \mathbf{F} - \mathbf{X}_{\mathrm{in}} \|_F^2}_{f(\mathbf{F})} \\ & \| \tilde{\Delta} \mathbf{F} \|_1 = \sum_{(v_i, v_j) \in \mathcal{E}} \left\| \frac{\mathbf{F}_i}{\sqrt{d_i + 1}} - \frac{\mathbf{F}_j}{\sqrt{d_j + 1}} \right\|_1 \end{aligned}$$
$$\begin{aligned} \mathbf{Option II} \\ & \underset{\mathbf{F} \in \mathbb{R}^{n \times d}}{\operatorname{arg min}} \underbrace{\lambda_1 \| \tilde{\Delta} \mathbf{F} \|_{21}}_{g_{21}(\tilde{\Delta} \mathbf{F})} + \underbrace{\frac{\lambda_2}{2} \operatorname{tr}(\mathbf{F}^\top \tilde{\mathbf{L}} \mathbf{F}) + \frac{1}{2} \| \mathbf{F} - \mathbf{X}_{\mathrm{in}} \|_F^2}_{f(\mathbf{F})} \\ & \| \tilde{\Delta} \mathbf{F} \|_{21} = \sum_{(v_i, v_j) \in \mathcal{E}} \left\| \frac{\mathbf{F}_i}{\sqrt{d_i + 1}} - \frac{\mathbf{F}_j}{\sqrt{d_j + 1}} \right\|_2 \end{aligned}$$

Define Prior  $\implies$  Optimization Solver  $\implies$  Message Passing

#### Data Science and Engineering Lab



### Elastic Graph Signal Estimator

$$\underset{\mathbf{F}\in\mathbb{R}^{n\times d}}{\arg\min}\underbrace{\lambda_{1}\|\tilde{\Delta}\mathbf{F}\|_{21}}_{g_{21}(\tilde{\Delta}\mathbf{F})} + \underbrace{\frac{\lambda_{2}}{2}\mathrm{tr}(\mathbf{F}^{\top}\tilde{\mathbf{L}}\mathbf{F}) + \frac{1}{2}\|\mathbf{F}-\mathbf{X}_{\mathrm{in}}\|_{F}^{2}}_{f(\mathbf{F})}$$

#### **Saddle-point reformulation**

$$\min_{\mathbf{F}} \max_{\mathbf{Z}} f(\mathbf{F}) + \langle \tilde{\Delta} \mathbf{F}, \mathbf{Z} \rangle - g^*(\mathbf{Z}) \qquad g^*(\mathbf{Z}) := \sup_{\mathbf{X}} \langle \mathbf{Z}, \mathbf{X} \rangle - g(\mathbf{X})$$

A simple and efficient primal dual solver

$$\begin{cases} \bar{\mathbf{F}}^{k+1} &= \mathbf{F}^k - \gamma \nabla f(\mathbf{F}^k) - \gamma \tilde{\Delta}^\top \mathbf{Z}^k, \\ \mathbf{Z}^{k+1} &= \mathbf{prox}_{\beta g^*} (\mathbf{Z}^k + \beta \tilde{\Delta} \bar{\mathbf{F}}^{k+1}), \\ \mathbf{F}^{k+1} &= \mathbf{F}^k - \gamma \nabla f(\mathbf{F}^k) - \gamma \tilde{\Delta}^\top \mathbf{Z}^{k+1}, \end{cases}$$



## Elastic Message Passing

$$\begin{cases} \mathbf{Y}^{k+1} = \gamma \mathbf{X}_{\text{in}} + (1-\gamma) \tilde{\mathbf{A}} \mathbf{F}^{k} \\ \bar{\mathbf{F}}^{k+1} = \mathbf{Y}^{k} - \gamma \tilde{\Delta}^{\top} \mathbf{Z}^{k} \\ \bar{\mathbf{Z}}^{k+1} = \mathbf{Z}^{k} + \beta \tilde{\Delta} \bar{\mathbf{F}}^{k+1} \\ \begin{cases} \mathbf{Z}^{k+1} = \min(|\bar{\mathbf{Z}}^{k+1}|, \lambda_{1}) \cdot \operatorname{sign}(\bar{\mathbf{Z}}^{k+1}) & (\text{Option I: } \ell_{1} \text{ norm}) \\ \mathbf{Z}_{i}^{k+1} = \min(||\bar{\mathbf{Z}}_{i}^{k+1}||_{2}, \lambda_{1}) \cdot \frac{\bar{\mathbf{Z}}_{i}^{k+1}}{\|\bar{\mathbf{Z}}_{i}^{k+1}\|_{2}}, \forall i \in [m] & (\text{Option II: } \ell_{21} \text{ norm}) \\ \mathbf{F}^{k+1} = \mathbf{Y}^{k} - \gamma \tilde{\Delta}^{\top} \mathbf{Z}^{k+1} \end{cases}$$

Figure 1. Elastic Message Passing (EMP).  $\mathbf{F}^0 = \mathbf{X}_{in}$  and  $\mathbf{Z}^0 = \mathbf{0}^{m \times d}$ .

#### Interpretation

- $\lambda_1 = 0$ : standard message passing in Y
  - $\gamma = \frac{1}{1+\lambda_2}, \ \lambda_2 = \frac{1}{\alpha} 1$ :  $\mathbf{F}^{k+1} = \alpha \mathbf{X}_{in} + (1-\alpha) \tilde{\mathbf{A}} \mathbf{F}^k$
  - $\gamma = \frac{1}{1+\lambda_2}$ ,  $\lambda_2 = +\infty$ :  $\mathbf{F}^{k+1} = \tilde{\mathbf{A}}\mathbf{F}^k$
- $\lambda_1 > 0$ : accumulate  $\widetilde{\Delta}^T Z$  to promote sparsity in  $\widetilde{\Delta}F$  and preserve jump edge



## Elastic Message Passing

$$\begin{cases} \mathbf{Y}^{k+1} = \gamma \mathbf{X}_{\text{in}} + (1-\gamma) \tilde{\mathbf{A}} \mathbf{F}^{k} \\ \bar{\mathbf{F}}^{k+1} = \mathbf{Y}^{k} - \gamma \tilde{\Delta}^{\top} \mathbf{Z}^{k} \\ \bar{\mathbf{Z}}^{k+1} = \mathbf{Z}^{k} + \beta \tilde{\Delta} \bar{\mathbf{F}}^{k+1} \\ \begin{cases} \mathbf{Z}^{k+1} = \min(|\bar{\mathbf{Z}}^{k+1}|, \lambda_{1}) \cdot \operatorname{sign}(\bar{\mathbf{Z}}^{k+1}) & (\text{Option I: } \ell_{1} \text{ norm}) \\ \mathbf{Z}_{i}^{k+1} = \min(||\bar{\mathbf{Z}}_{i}^{k+1}||_{2}, \lambda_{1}) \cdot \frac{\bar{\mathbf{Z}}_{i}^{k+1}}{\|\bar{\mathbf{Z}}_{i}^{k+1}\|_{2}}, \forall i \in [m] & (\text{Option II: } \ell_{21} \text{ norm}) \\ \mathbf{F}^{k+1} = \mathbf{Y}^{k} - \gamma \tilde{\Delta}^{\top} \mathbf{Z}^{k+1} \end{cases}$$

Figure 1. Elastic Message Passing (EMP).  $\mathbf{F}^0 = \mathbf{X}_{in}$  and  $\mathbf{Z}^0 = \mathbf{0}^{m \times d}$ .

#### Theorem (Convergence)

Under the stepsize setting  $\gamma < \frac{2}{1+\lambda_2 \|\tilde{\mathbf{L}}\|_2}$  and  $\beta \leq \frac{4}{3\gamma \|\tilde{\Delta}\tilde{\Delta}^\top\|_2}$ , the elastic message passing scheme (EMP) converges to the optimal solution of the elastic graph signal estimator. It is sufficient to choose any  $\gamma < \frac{2}{1+2\lambda_2}$  and  $\beta \leq \frac{2}{3\gamma}$  since  $\|\tilde{\mathbf{L}}\|_2 = \|\tilde{\Delta}^\top \tilde{\Delta}\|_2 = \|\tilde{\Delta}\tilde{\Delta}^\top\|_2 \leq 2$ .

In this work, we fix 
$$\gamma = \frac{1}{1+\lambda_2}$$
,  $\beta = \frac{1}{2\gamma}$ 



$$\mathbf{Y}_{\text{pre}} = \mathbf{EMP}\left(h_{\theta}(\mathbf{X}_{\text{fea}}), K, \lambda_{1}, \lambda_{2}\right)$$

- Follow the decoupled architecture as PPNP but can be used in coupled architecture as well
- EMP is composed by simple and efficient operations, which is friendly to efficient and back-propagation training
- Hyperparameters  $\lambda_1$  and  $\lambda_2$  provide better smoothness adaptivity
- Doesn't require a very large K



#### Semi-supervised learning for node classification

Table 1. Classification accuracy (%) on benchmark datasets with 10 times random data splits.

Model	Cora	CiteSeer	PubMed	CS	Physics	Computers	Photo
ChebNet	$76.3 \pm 1.5$	$67.4 \pm 1.5$	$75.0\pm2.0$	$91.8\pm0.4$	OOM	$\textbf{81.0} \pm \textbf{2.0}$	$90.4 \pm 1.0$
GCN	$79.6 \pm 1.1$	$68.9 \pm 1.2$	$77.6\pm2.3$	$91.6\pm0.6$	$93.3\pm0.8$	$79.8 \pm 1.6$	$90.3 \pm 1.2$
GAT	$80.1\pm1.2$	$68.9 \pm 1.8$	$77.6\pm2.2$	$91.1\pm0.5$	$93.3\pm0.7$	$79.3\pm2.4$	$89.6 \pm 1.6$
SGC	$80.2\pm1.5$	$68.9 \pm 1.3$	$75.5\pm2.9$	$90.1\pm1.3$	$93.1\pm0.6$	$73.0\pm2.0$	$83.5\pm2.9$
APPNP	$82.2\pm1.3$	$70.4 \pm 1.2$	$78.9\pm2.2$	$\textbf{92.5} \pm \textbf{0.3}$	$93.7\pm0.7$	$80.1\pm2.1$	$90.8 \pm 1.3$
GraphSAGE	$79.0 \pm 1.1$	$67.5\pm2.0$	$77.6\pm2.0$	$91.7\pm0.5$	$92.5\pm0.8$	$80.7\pm1.7$	$90.9 \pm 1.0$
ElasticGNN	$\textbf{82.7} \pm \textbf{1.0}$	$\textbf{70.9} \pm \textbf{1.4}$	$\textbf{79.4} \pm \textbf{1.8}$	$\textbf{92.5} \pm \textbf{0.3}$	$\textbf{94.2} \pm \textbf{0.5}$	$80.7\pm1.8$	$\textbf{91.3} \pm \textbf{1.3}$

ElasticGNN: L<sub>21</sub>+L<sub>2</sub>





#### Better local smoothness adaptivity

*Table 3.* Ratio between average node differences along wrong and correct edges.

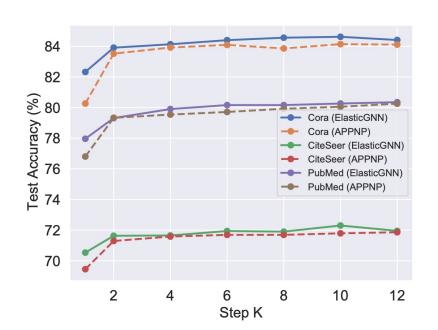
Model	Cora	CiteSeer	PubMed	
$\ell_2$ (APPNP)	1.57	1.35	1.43	
$\ell_{21}$ + $\ell_2$ (ElasticGNN)	2.03	1.94	1.79	

#### **Piecewise constant prior**

*Table 4.* Sparsity ratio (i.e.,  $\|(\tilde{\Delta}\mathbf{F})_i\|_2 < 0.1$ ) in node differences  $\tilde{\Delta}\mathbf{F}$ .

Model	Cora	CiteSeer	PubMed
$\ell_2$ (APPNP)	2%	16%	11%
$\ell_{21}$ + $\ell_2$ (ElasticGNN)	37%	74%	42%

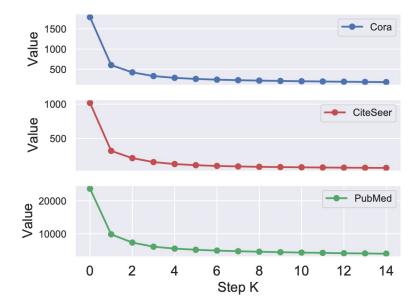
### Performance on benchmark datasets



Impact of K

Figure 2. Classification accuracy under different propagation steps.

#### **Convergence of EMP**



*Figure 3.* Convergence of the objective value for the problem in Eq. (8) during message passing.



### Performance under adversarial attack

Deteret	Ptb Rate	Basic GNN		Elastic GNN					
Dataset		GCN	GAT	$\ell_2$	$\ell_1$	$\ell_{21}$	$\ell_1 + \ell_2$	$\ell_{21} + \ell_2$	
	0%	83.5±0.4	84.0±0.7	85.8±0.4	85.1±0.5	85.3±0.4	85.8±0.4	85.8±0.4	
	5%	$76.6{\pm}0.8$	$80.4 {\pm} 0.7$	$81.0{\pm}1.0$	82.3±1.1	$81.6 \pm 1.1$	$81.9 {\pm} 1.4$	82.2±0.9	
Cora	10%	$70.4 \pm 1.3$	$75.6 {\pm} 0.6$	$76.3 \pm 1.5$	$76.2 \pm 1.4$	$77.9{\pm}0.9$	$78.2 \pm 1.6$	78.8±1.7	
Cora	15%	$65.1 \pm 0.7$	69.8±1.3	$72.2 \pm 0.9$	$73.3 \pm 1.3$	$75.7 \pm 1.2$	$76.9{\pm}0.9$	77.2±1.6	
	20%	$60.0{\pm}2.7$	59.9±0.6	67.7±0.7	$63.7{\pm}0.9$	$70.3 \pm 1.1$	$67.2 \pm 5.3$	70.5±1.3	
	0%	72.0±0.6	73.3±0.8	73.6±0.9	73.2±0.6	$73.2{\pm}0.5$	73.6±0.6	73.8±0.6	
	5%	$70.9{\pm}0.6$	$72.9{\pm}0.8$	$72.8 {\pm} 0.5$	$72.8{\pm}0.5$	$72.8{\pm}0.5$	73.3±0.6	$72.9{\pm}0.5$	
Citeseer	10%	$67.6 {\pm} 0.9$	$70.6 \pm 0.5$	$70.2 \pm 0.6$	$70.8{\pm}0.6$	$70.7 \pm 1.2$	$72.4 {\pm} 0.9$	72.6±0.4	
Cileseer	15%	$64.5 \pm 1.1$	69.0±1.1	$70.2 \pm 0.6$	68.1±1.4	$68.2 \pm 1.1$	$71.3 \pm 1.5$	71.9±0.7	
	20%	62.0±3.5	61.0±1.5	64.9±1.0	$64.7{\pm}0.8$	64.7±0.8	$64.7{\pm}0.8$	64.7±0.8	
	0%	95.7±0.4	95.4±0.2	95.4±0.2	95.8±0.3	95.8±0.3	95.8±0.3	95.8±0.3	
	5%	$73.1{\pm}0.8$	83.7±1.5	$82.8 {\pm} 0.3$	$78.7{\pm}0.6$	$78.7{\pm}0.7$	$82.8{\pm}0.4$	83.0±0.3	
Dalblags	10%	$70.7 \pm 1.1$	$76.3 {\pm} 0.9$	73.7±0.3	$75.2 {\pm} 0.4$	$75.3 {\pm} 0.7$	$81.5 {\pm} 0.2$	81.6±0.3	
Polblogs	15%	$65.0 \pm 1.9$	$68.8 {\pm} 1.1$	$68.9 \pm 0.9$	$72.1 {\pm} 0.9$	$71.5 \pm 1.1$	$77.8{\pm}0.9$	78.7±0.5	
	20%	$51.3 \pm 1.2$	$51.5 \pm 1.6$	$65.5 \pm 0.7$	68.1±0.6	$68.7{\pm}0.7$	$77.4{\pm}0.2$	77.5±0.2	
	0%	87.2±0.1	83.7±0.4	88.1±0.1	86.7±0.1	87.3±0.1	88.1±0.1	88.1±0.1	
	5%	83.1±0.1	$78.0{\pm}0.4$	87.1±0.2	$86.2 {\pm} 0.1$	$87.0 {\pm} 0.1$	87.1±0.2	87.1±0.2	
Pubmed	10%	$81.2{\pm}0.1$	$74.9{\pm}0.4$	86.6±0.1	$86.0{\pm}0.2$	$86.9{\pm}0.2$	86.3±0.1	87.0±0.1	
	15%	$78.7{\pm}0.1$	$71.1 \pm 0.5$	85.7±0.2	$85.4{\pm}0.2$	$86.4 {\pm} 0.2$	$85.5{\pm}0.1$	86.4±0.2	
	20%	77.4±0.2	68.2±1.0	85.8±0.1	$85.4{\pm}0.1$	86.4±0.1	$85.4{\pm}0.1$	86.4±0.1	

*Table 2.* Classification accuracy (%) under different perturbation rates of adversarial graph attack.

#### Basic GNNs < Elastic GNNs



### Performance under adversarial attack

Dataset	Dth Data	Basic GNN		Elastic GNN					
Dalasel	Ptb Rate	GCN	GAT	$\ell_2$	$\ell_1$	$\ell_{21}$	$\ell_1 + \ell_2$	$\ell_{21} + \ell_2$	
	0%	83.5±0.4	84.0±0.7	85.8±0.4	85.1±0.5	85.3±0.4	85.8±0.4	85.8±0.4	
	5%	$76.6 {\pm} 0.8$	$80.4{\pm}0.7$	$81.0{\pm}1.0$	82.3±1.1	81.6±1.1	$81.9{\pm}1.4$	$82.2{\pm}0.9$	
Cora	10%	$70.4 \pm 1.3$	$75.6{\pm}0.6$	$76.3 \pm 1.5$	$76.2 \pm 1.4$	77.9±0.9	$78.2 \pm 1.6$	78.8±1.7	
Cola	15%	65.1±0.7	$69.8 {\pm} 1.3$	$72.2 \pm 0.9$	$73.3 {\pm} 1.3$	75.7±1.2	$76.9{\pm}0.9$	77.2±1.6	
	20%	$60.0 \pm 2.7$	$59.9{\pm}0.6$	67.7±0.7	$63.7{\pm}0.9$	70.3±1.1	$67.2\pm5.3$	70.5±1.3	
	0%	72.0±0.6	73.3±0.8	73.6±0.9	73.2±0.6	73.2±0.5	73.6±0.6	73.8±0.6	
	5%	70.9±0.6	$72.9{\pm}0.8$	$72.8 {\pm} 0.5$	$72.8{\pm}0.5$	72.8±0.5	73.3±0.6	$72.9{\pm}0.5$	
Citagoan	10%	67.6±0.9	$70.6{\pm}0.5$	$70.2 \pm 0.6$	$70.8{\pm}0.6$	70.7±1.2	$72.4 {\pm} 0.9$	72.6±0.4	
Citeseer	15%	64.5±1.1	$69.0 \pm 1.1$	$70.2 \pm 0.6$	68.1±1.4	68.2±1.1	$71.3 \pm 1.5$	71.9±0.7	
	20%	62.0±3.5	$61.0{\pm}1.5$	64.9±1.0	$64.7{\pm}0.8$	64.7±0.8	$64.7{\pm}0.8$	$64.7{\pm}0.8$	
	0%	95.7±0.4	95.4±0.2	95.4±0.2	95.8±0.3	95.8±0.3	95.8±0.3	95.8±0.3	
	5%	73.1±0.8	83.7±1.5	$82.8{\pm}0.3$	$78.7{\pm}0.6$	78.7±0.7	$82.8{\pm}0.4$	83.0±0.3	
Dalblaga	10%	$70.7 \pm 1.1$	$76.3{\pm}0.9$	73.7±0.3	$75.2{\pm}0.4$	75.3±0.7	$81.5 {\pm} 0.2$	81.6±0.3	
Polblogs	15%	65.0±1.9	$68.8 {\pm} 1.1$	$68.9 \pm 0.9$	$72.1 {\pm} 0.9$	$71.5 \pm 1.1$	$77.8{\pm}0.9$	78.7±0.5	
	20%	$51.3 \pm 1.2$	$51.5{\pm}1.6$	$65.5 \pm 0.7$	$68.1{\pm}0.6$	68.7±0.7	$77.4{\pm}0.2$	$77.5 {\pm} 0.2$	
	0%	87.2±0.1	83.7±0.4	88.1±0.1	86.7±0.1	87.3±0.1	88.1±0.1	88.1±0.1	
Pubmed	5%	83.1±0.1	$78.0{\pm}0.4$	87.1±0.2	$86.2{\pm}0.1$	87.0±0.1	87.1±0.2	87.1±0.2	
	10%	81.2±0.1	$74.9{\pm}0.4$	86.6±0.1	$86.0{\pm}0.2$	86.9±0.2	86.3±0.1	87.0±0.1	
	15%	78.7±0.1	$71.1 {\pm} 0.5$	85.7±0.2	$85.4{\pm}0.2$	86.4±0.2	$85.5 {\pm} 0.1$	86.4±0.2	
	20%	$77.4 \pm 0.2$	$68.2{\pm}1.0$	85.8±0.1	$85.4{\pm}0.1$	86.4±0.1	$85.4{\pm}0.1$	86.4±0.1	

Table 2. Classification accuracy (%) under different perturbation rates of adversarial graph attack.

 $L_2 < L_{21}$  in most cases



### Performance under adversarial attack

Dataset	Ptb Rate	Basic GNN		Elastic GNN					
Dataset		GCN	GAT	$\ell_2$	$\ell_1$	$\ell_{21}$	$\ell_1 + \ell_2$	$\ell_{21} + \ell_2$	
	0%	83.5±0.4	84.0±0.7	85.8±0.4	85.1±0.5	85.3±0.4	85.8±0.4	85.8±0.4	
	5%	$76.6 {\pm} 0.8$	$80.4{\pm}0.7$	81.0±1.0	82.3±1.1	$81.6 {\pm} 1.1$	$81.9{\pm}1.4$	82.2±0.9	
Cora	10%	$70.4 \pm 1.3$	$75.6{\pm}0.6$	$76.3 \pm 1.5$	$76.2 \pm 1.4$	$77.9{\pm}0.9$	$78.2{\pm}1.6$	78.8±1.7	
Cola	15%	65.1±0.7	$69.8 {\pm} 1.3$	$72.2 \pm 0.9$	$73.3 {\pm} 1.3$	$75.7 \pm 1.2$	$76.9{\pm}0.9$	77.2±1.6	
	20%	$60.0{\pm}2.7$	$59.9{\pm}0.6$	67.7±0.7	$63.7{\pm}0.9$	$70.3 \pm 1.1$	$67.2\pm5.3$	70.5±1.3	
	0%	72.0±0.6	73.3±0.8	73.6±0.9	73.2±0.6	73.2±0.5	73.6±0.6	73.8±0.6	
	5%	70.9±0.6	$72.9{\pm}0.8$	$72.8 \pm 0.5$	$72.8{\pm}0.5$	$72.8{\pm}0.5$	73.3±0.6	72.9±0.5	
Citeseer	10%	67.6±0.9	$70.6 \pm 0.5$	$70.2 \pm 0.6$	$70.8{\pm}0.6$	$70.7 \pm 1.2$	72.4±0.9	72.6±0.4	
Citeseer	15%	$64.5 \pm 1.1$	$69.0 \pm 1.1$	$70.2 \pm 0.6$	68.1±1.4	$68.2 \pm 1.1$	$71.3 \pm 1.5$	71.9±0.7	
	20%	$62.0 \pm 3.5$	$61.0{\pm}1.5$	64.9±1.0	$64.7{\pm}0.8$	$64.7{\pm}0.8$	$64.7{\pm}0.8$	64.7±0.8	
	0%	95.7±0.4	95.4±0.2	95.4±0.2	95.8±0.3	95.8±0.3	95.8±0.3	95.8±0.3	
	5%	73.1±0.8	83.7±1.5	82.8±0.3	$78.7{\pm}0.6$	$78.7{\pm}0.7$	82.8±0.4	83.0±0.3	
Dalblaga	10%	$70.7 \pm 1.1$	$76.3{\pm}0.9$	73.7±0.3	$75.2{\pm}0.4$	$75.3 {\pm} 0.7$	81.5±0.2	81.6±0.3	
Polblogs	15%	65.0±1.9	$68.8 {\pm} 1.1$	$68.9 \pm 0.9$	$72.1 {\pm} 0.9$	$71.5 \pm 1.1$	$77.8 \pm 0.9$	78.7±0.5	
	20%	51.3±1.2	$51.5 \pm 1.6$	$65.5 \pm 0.7$	$68.1 \pm 0.6$	$68.7{\pm}0.7$	$77.4{\pm}0.2$	77.5±0.2	
	0%	87.2±0.1	83.7±0.4	88.1±0.1	86.7±0.1	87.3±0.1	88.1±0.1	88.1±0.1	
	5%	83.1±0.1	$78.0{\pm}0.4$	87.1±0.2	$86.2 {\pm} 0.1$	$87.0 {\pm} 0.1$	87.1±0.2	87.1±0.2	
Pubmed	10%	81.2±0.1	$74.9{\pm}0.4$	86.6±0.1	$86.0\pm0.2$	86.9±0.2	86.3±0.1	87.0±0.1	
	15%	78.7±0.1	$71.1 {\pm} 0.5$	85.7±0.2	$85.4{\pm}0.2$	86.4±0.2	85.5±0.1	86.4±0.2	
	20%	77.4±0.2	68.2±1.0	85.8±0.1	$85.4{\pm}0.1$	86.4±0.1	85.4±0.1	86.4±0.1	

Table 2. Classification accuracy (%) under different perturbation rates of adversarial graph attack.

 $L_1 + L_2 < L_{21} + L_2$  in most cases





## Conclusion

#### Summary

- Introduce  $L_1$  based graph smoothing in the design of GNNs, for the first time
- Derive a novel and general message passing scheme, i.e., EMP
- Develop a family of GNNs, i.e., Elastic GNNs
- Demonstrate better smoothness adaptivity of Elastic GNNs
- Elastic GNNs are intrinsically more robust to adversarial graph attacks and compatible with any other defense strategies

#### **Future directions**

- Other node level tasks such as link prediction, community detection, and outlier detection
- Graph level tasks such as graph classification and graph similarity measure
- Higher-order graph difference operators
- EMP as a building block in other GNN architectures

Code: https://github.com/lxiaorui/ElasticGNN



### Thanks for the funding support from National Science Founding (NSF), Army Research Office (ARO) and Facebook Faculty Research Award.







