DISTRIBUTIONALLY ROBUST SEMI-SUPERVISED LEARNING OVER GRAPHS

Alireza Sadeghi, Meng Ma, Bingcong Li, Georgios B. Giannakis
Department of ECE and Digital Technology Center
University of Minnesota
Minneapolis, MN 55455, USA
{sadeg012, maxxx971, lixx5599, georgios}@umn.edu

ABSTRACT

Semi-supervised learning (SSL) over graph-structured data emerges in many network science applications. To efficiently manage learning over graphs, variants of graph neural networks (GNNs) have been developed recently. By succinctly encoding local graph structures and features of nodes, state-of-the-art GNNs can scale linearly with the size of graph. Despite their success in practice, most of existing methods are unable to handle graphs with uncertain nodal attributes. Specifically whenever mismatches between training and testing data distribution exists, these models fail in practice. Challenges also arise due to distributional uncertainties associated with data acquired by noisy measurements. In this context, a distributionally robust learning framework is developed, where the objective is to train models that exhibit quantifiable robustness against perturbations. The data distribution is considered unknown, but lies within a Wasserstein ball centered around empirical data distribution. A robust model is obtained by minimizing the worst expected loss over this ball. However, solving the emerging functional optimization problem is challenging, if not impossible. Advocating a strong duality condition, we develop a principled method that renders the problem tractable and efficiently solvable. Experiments assess the performance of the proposed method.

1 INTRODUCTION

Relations among data in real world applications can often be captured by graphs, for instance the analysis and inference tasks for social, brain, communication, biological, transportation, and sensor networks (Shuman et al., 2013; Kolaczyk & Csárdi, 2014). In practice however, the data is only available for a subset of nodes, due to for example the cost, and computational or privacy constraints. Most of these applications however, deal with inference of processes across all the network nodes. Such semi-supervised learning (SSL) tasks over networks can be addressed by exploiting the underlying graph topology (Chapelle et al., 2009).

Graph neural networks (GNNs) are parametric models that combine graph-filters and topology information with point-wise nonlinearities, to form nested architectures to easily express the functions defined over graphs (Zhou et al., 2018). By exploiting the underlying irregular structure of network data, the GNNs enjoy lower computational complexity, less parameters for training, and improved generalization capabilities relative to traditional deep neural networks (DNNs), making them appealing for learning over graphs (Zhou et al., 2018; Wu et al., 2020; Gama et al., 2019).

Similar to other DNN models, GNNs are also susceptible to adversarial manipulated input data or, distributional uncertainties, such as mismatches between training and testing data distributions. For instance small perturbations to input data would significantly deteriorate the regression performance, or result in classification error (Zügner et al., 2020; Jin et al., 2020), just to name a few. Hence, it is critical to develop principled methods that can endow GNNs with robustness, especially in safety-critical applications, such as robotics (Tolstaya et al., 2020), and transportation (Zhou et al., 2020).

Contributions. This paper endows SSL over graphs using GNNs with robustness against distributional uncertainties and possibly adversarial perturbations. Assuming the data distribution lies inside a Wasserstein ball centered at empirical data distribution, we robustify the model by minimizing the...
worst expected loss over the considered ball, which is challenging to solve. Invoking recently developed strong duality results, we develop an equivalent unconstrained and tractable learning problem.

1.1 Problem formulation

Consider a SSL task over a graph $\mathcal{G} := \{\mathcal{V}, \mathbf{W}\}$ with $N$ nodes, where $\mathcal{V} := \{1, \ldots, N\}$ denotes the vertex set, and $\mathbf{W}$ represents the $N \times N$ weighted adjacency matrix capturing node connectivity. The associated unnormalized graph Laplacian matrix of the undirected graph $\mathcal{G}$ is $\mathbf{L} := \mathbf{D} - \mathbf{A}$, where $\mathbf{D} := \text{diag}\{\mathbf{W} 1_N\}$, with $1_N$ denoting the $N \times 1$ all-one column vector. Denote by matrix $\mathbf{X}_s \in \mathbb{R}^{N \times F}$ the nodal feature vectors sampled at instances $s = 1, 2, \ldots$, with $n$-th row $\mathbf{x}_{n,s} := [\mathbf{X}_s]_{n,:}$, representing a feature vector of length $F$ associated with node $n \in \mathcal{V}$, and $\top$ stands for transposition. In the given graph, the labels $\{y_{n,s}\}_{n \in \mathcal{O}_s}$ are given for only a small subset of nodes, where $\mathcal{O}_s$ represents the index set of observed nodes sampled at $s$, and $\mathcal{U}_s$ the index set of unobserved nodes.

Given $\{\mathbf{X}_s, y_s\}$, where $y_s$ is the vector of observed labels, the goal is to find the labels of unobserved nodes $\{y_{n,s}\}_{n \in \mathcal{U}_s}$. To this aim our objective is to learn a functional mapping $f(\mathbf{X}_s; \mathbf{W})$ that can infer the missing labels based on available information. Such a function can be learned by solving the following optimization problem (see e.g., Kipf & Welling [2016] for more details)

$$
\min_{f \in \mathcal{F}} \mathbb{E}_{(n,s) \sim P_s} \left[ \sum_{n \in \mathcal{O}_s} ||f(\mathbf{x}_n; \mathbf{W}) - y_n||^2 + \lambda \sum_{n,n'} ||f(\mathbf{x}_n; \mathbf{W}) - f(\mathbf{x}_{n'}; \mathbf{W})||^2 \right],
$$

(1)

where $\mathcal{L}_0$ represents the supervised loss w.r.t. the observed part of the graph, $\mathcal{L}_{\text{reg}}$ represents the Laplacian regularization term, $\mathcal{F}$ denotes the feasible set of functions that we can learn, and $\lambda \geq 0$ is a hyper parameter. The regularization term relies on the premise that connected nodes in the graph are likely to share similar labels. The expectation here is taken with respect to (w.r.t) the feature and label data generating distribution.

In this work, we first encode the graph structure using a GNN model denoted by $f(\mathbf{X}; \theta, \mathbf{W})$, where $\theta$ represents the model parameters. Such a parametric representation enables bypassing explicit graph-based regularization $\mathcal{L}_{\text{reg}}$ represented in (1). The GNN model of $f(\cdot)$ relies on the weighted adjacency $\mathbf{W}$ and therefore can easily propagate information from observed nodes $\mathcal{O}_s$ to unobserved ones $\mathcal{U}_s$. In a nutshell, objective is to learn a parametric model by solving the following problem

$$
\min_{\theta \in \Theta} \mathbb{E}_{(\mathbf{x},y) \sim P_0} \mathcal{L}_0(f(\mathbf{X}; \theta; \mathbf{W}), y)
$$

(2)

where $\Theta$ is a feasible set, and $P_0$ is the feature and label data generating distribution. Despite restricting the modeling capacity through parameterizing $f(\cdot)$ with GNNs, we may inflict additional prior information into the sought formulation through exploiting the weighted adjacency matrix $\mathbf{W}$, which does not necessarily encode node similarities.

In practice, $P_0$ is typically unknown, instead some data samples $\{\mathbf{X}_s, y_s\}_{s=1}^S$ are given. Upon replacing the nominal distribution with an empirical one, we arrive at the empirical loss minimization problem, that is $\min_{\theta \in \Theta} S^{-1} \sum_{s=1}^S \mathcal{L}_0(f(\mathbf{X}_s; \theta; \mathbf{W}), y_s)$. The model obtained by solving empirical risk minimization does not exhibit any robustness in practice, specifically if there is any mismatch between the training and testing data distributions. To endow robustness, we reformulate this learning problem in a fresh manner as described in ensuing section.

2 Distributionally Robust Learning

To endow robustness, we consider the following optimization problem

$$
\min_{\theta \in \Theta} \sup_{\mathcal{P} \in \mathcal{P}} \mathbb{E}_{(\mathbf{x},y) \sim \mathcal{P}} \mathcal{L}_0(f(\mathbf{X}; \theta; \mathbf{W}), y)
$$

(3)

where $\mathcal{P}$ is a set of distributions centered around the empirical data distribution $\hat{P}_0$. This novel reformulation in (3) yields a model that performs reasonably well among a continuum of distributions. Various ambiguity sets $\mathcal{P}$ can be considered in practice, and they lead to different robustness guarantees with different computational requirements. For instance momentum, KL divergence, statistical test, and Wasserstein distance-based sets are popular in practice; see also Blanchet & Murthy [2019].
To formalize our framework, let us first define the Wasserstein distance between two probability measures. To this aim, consider probability measures $P$ and $\hat{P}$ supported on some set $X$, and let $\Pi(P, \hat{P})$ denote the set of joint measures (a.k.a coupling) defined over $X \times \hat{X}$, with marginals $P$ and $\hat{P}$, and let $c : X \times \hat{X} \to [0, \infty)$ measure the transportation cost for a unit of mass from $X \in X'$ in $P$ to $X' \in \hat{P}$. The so-called optimal transport problem is concerned with the minimum cost associated with transporting all the mass from $P$ to $\hat{P}$ through finding the optimal coupling, i.e., $W_c(P, \hat{P}) := \inf_{\pi \in \Pi} \mathbb{E}_\pi[c(X, X')]$. If $c(\cdot, \cdot)$ satisfies the axioms of distance, then $W_c$ defines a distance on the space of probability measures. For instance, if $P$ and $\hat{P}$ are defined over a Polish space equipped with metric $d$, then fixing $c(X, X') = d^p(X, X')$ for some $p \in [1, \infty)$ asserts that $W^{1/p}_c(P, \hat{P})$ is the well-known Wasserstein distance of order $p$ between $P$ and $\hat{P}$.

Using the Wasserstein distance, let us define the uncertainty set $\mathcal{P} := \{P | W_c(P, \hat{P}_0) \leq \rho\}$ to include all probability distribution functions (pdfs) having at most $\rho$-distance from $\hat{P}_0$. Incorporating this ambiguity set into \cite{sinha2017} the following robust surrogate is considered in this work

$$\min_{\theta \in \Theta} \sup_{P \in \mathcal{P}} \mathbb{E}_{(X, Y) \sim P} \mathcal{L}_0(f(X, \theta; W), y), \quad \text{where } \mathcal{P} := \left\{P | W_c(P, \hat{P}_0) \leq \rho\right\}. \quad (4)$$

The inner supremum here goes after pdfs characterized by $P$. Solving this optimization directly over the infinite-dimensional space of distribution functions raises practical challenges. Fortunately, under some mild conditions over losses as well as transport costs, the inner maximization satisfies a strong duality condition (see Blanchet et al. \citeyear{blanchet2006} for a detailed discussions), which means the optimal objective of this inner maximization and its Lagrangian dual are equal. Enticingly, the dual reformulation involves optimization over only one-dimensional dual variable. These properties make it practically appealing to solve \cite{blanchet2019} directly in the dual domain. The following proposition highlights the strong duality result, whose proofs can be found in Blanchet & Murthy \citeyear{blanchet2019}.

**Proposition 1** Under some mild conditions over the loss $\mathcal{L}_0(\cdot)$ and cost $c(\cdot)$, it holds that

$$\sup_{P \in \mathcal{P}} \mathbb{E}_P \mathcal{L}_0(f(X, \theta; W), y) = \inf_{\gamma \geq 0} \sum_{s=1}^S \sup_{\xi \in X} \mathcal{L}_0(f(\xi, \theta; W), y_s) + \gamma(\rho - c(X_s, \xi)) \quad (5)$$

where $\mathcal{P} := \left\{P | W_c(P, \hat{P}_0) \leq \rho\right\}$.

The right-hand side in \cite{blanchet2019} simply is the univariate dual reformulation of the primal problem represented in the left-hand side. Furthermore, different from the primal formulation, the expectation in the dual domain is replaced with the summation over available training data, rather than any $P \in \mathcal{P}$ that needs to be obtained by solving for the optimal $\pi \in \Pi$ to form $P$. Because of these two properties, solving the dual problem is practically more appealing. Thus, hinging on Proposition 1 the following distributionally robust surrogate is considered in this work

$$\min_{\theta \in \Theta} \inf_{\gamma \geq 0} \sum_{s=1}^S \sup_{\xi \in X} \mathcal{L}_0(f(\xi, \theta; W), y_s) + \gamma(\rho - c(X_s, \xi)) \quad (6)$$

This problem requires the supremum to be solved separately for each sample $X_s$, which cannot be handled through existing methods. Our approach to address this relies on the structure of this problem to *iteratively* update parameters $\tilde{\theta} := [\theta^\top, \gamma^\top]^\top$ and $\xi$, Specifically, we rely on Danskin’s theorem to first maximize over $\xi$, which results in a differentiable function of $\theta$, and then minimize the objective w.r.t. $\theta$ using gradient descent. However, to guarantee convergence to a stationary point and utilize Danskin’s theorem, we need to make sure the inner maximization admits a unique solution (singleton). By choosing a strongly convex transportation cost such as $c(X, \xi) := \|X - $
Figure 1: Performance during testing for both normal (a) - (b), and perturbed input features (c) - (d).

\[ \xi^2 \gamma, \text{ and by selecting } \gamma \in \Gamma := \{ \gamma | \gamma > \gamma_0 \} \text{ with a large enough } \gamma_0, \text{ we arrive at a strongly concave objective function for the maximization over } \xi. \text{ Since } \gamma \text{ is the dual variable associated with the constraint in (6) having } \gamma \in \Gamma \text{ is tantamount to tuning } \rho, \text{ which in turn controls the level of robustness. Replacing } \gamma \geq 0 \text{ in (6) with } \gamma \in \Gamma, \text{ our robust model can be obtained as the solution of}

\begin{equation}
\min_{\theta \in \Theta} \inf_{\gamma \in \Gamma} \sup_{s} \psi(\tilde{\theta}, \xi; X_s)
\end{equation}

where \( \psi(\tilde{\theta}, \xi; X_s) = \mathcal{L}_0(f(\xi, \theta; W), y_s) + \gamma (\rho - c(X_s, \xi)) \). Intuitively, input \( X_s \) in (7) is preprocessed by maximizing \( \psi(\cdot) \) accounting for a perturbation. We iteratively solve (7) after sampling a mini-batch of data, we first pre-process them by maximizing the function \( \psi(\cdot) \). Then, we use a simple gradient descent to update \( \tilde{\theta} \). Notice that the \( \theta \) inside function \( \psi(\cdot) \), represents the weights of our considered GNN, whose details are provided in the Appendix. A promising future research direction is to optimally/adaptively tune the hyper parameter \( \rho \). We refer interested readers to Esfahani & Kuhn [2018], Fourner & Guilin [2015] for further discussions.

3 EXPERIMENTS

The performance of our novel distributionally robust GNN-based SSL is tested in a regression task using real load consumption data from the 2012 Global Energy Forecasting Competition (GEFC). Our objective here is to estimate only the amplitudes of voltages across all the nodes in a standard IEEE 118-bus network. Utilizing this data set, the training and testing data are prepared by solving the so-called AC power flow equations using the MATPOWER toolbox (Zimmerman et al., 2010).

The measurements \( X \) used include all active and reactive power injections, corrupted by small additive white Gaussian noise. Using MATPOWER we generated 1,000 pairs of measurements and ground-truth voltages. We used 80% of this data for training and the remaining for testing. Throughout the training, the Adam optimizer with a fixed learning rate \( 10^{-3} \) was employed to minimize the Huber loss. Furthermore, the batch size was set to 32 during all 100 epochs.

To compare our method we employed 3 different benchmarks, namely: i) the prox-linear network introduced in Zhang et al. [2019]; ii) a 6-layer vanilla feed-forward neural network (FNN); and, iii) an 8-layer FNN. Our considered GNN uses \( K = 2 \) with \( D = 8 \) hidden units with ReLU activation.

The first set of tests are carried out using normal (not-corrupted) data, where the results are depicted in Fig. 1. Here we show the estimated (normalized) voltage amplitudes at different nodes, namely 105, and 20 during the given time course. The black curve represents the ground truth signal to be estimated. Clearly our GNN-based method outperforms alternative methods.

The second set of experiments are carried out over corrupted input signals, and the results are reported in Fig. 1. Specifically the training samples were generated according to \( P_b \), but during testing samples were perturbed to satisfy the constraint \( P \in \mathcal{P} \), that would yield the worst expected loss. Fig. 1 depicts the estimated signals across nodes 40 and 90. Here we fixed \( \rho = 10 \) and related hyper-parameters are tuned using grid search. As the plots showcase, the our proposed GNN-based robust method outperforms competing alternatives with corrupted inputs.

4 CONCLUSIONS

This contribution dealt with semi-supervised learning over graphs using GNNs. To account for uncertainties associated with data distributions, or adversarially manipulated input data, a principled robust learning framework was developed. Using the parametric models, we were able to reconstruct the unobserved nodal values.
REFERENCES

J. Blanchet and K. Murthy. Quantifying distributional model risk via optimal transport. *Math. Oper. Res.*, 44:565–600, 2019.

J. Blanchet, Y. Kang, F. Zhang, and K. Murthy. Data-driven optimal transport cost selection for distributionally robust optimization. *Stat.*, 1050:1527–1554, 2006.

O. Chapelle, B. Scholkopf, and A. Zien. Semi-supervised learning. *IEEE Trans. Neural Netw.*, 3:542, 2009.

P. M. Esfahani and D. Kuhn. Data-driven distributionally robust optimization using the Wasserstein metric: Performance guarantees and tractable reformulations. *Math. Prog.*, 171(1):115–166, 2018.

N. Fournier and A. Guillin. On the rate of convergence in Wasserstein distance of the empirical measure. *Probability Theory and Related Fields*, 162(3):707–738, 2015.

F. Gama, A. G. Marques, G. Leus, and A. Ribeiro. Convolutional neural network architectures for signals supported on graphs. *IEEE Trans. Signal Process.*, 67:1034–1049, 2019.

W. Jin, Y. Li, H. Xu, Y. Wang, and J. Tang. Adversarial attacks and defenses on graphs: A review and empirical study. *arXiv:2003.00653*, 2020.

T. N. Kipf and M. Welling. Semi-supervised classification with graph convolutional networks. *Intl. Conf. Lear. Rep.*, 2016.

E. D. Kolaczyk and G. Csárdi. *Statistical analysis of network data with R*, volume 65. Springer, 2014.

D. I. Shuman, S. K. Narang, P. Frossard, A. Ortega, and P. Vandergheynst. The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains. *IEEE Signal Process. Mag.*, 30:83–98, 2013.

A. Sinha, H. Namkoong, and R. Volpiand J. Duchi. Certifying some distributional robustness with principled adversarial training. *Intl. Conf. Lear. Rep.*, 2017.

E. Tolstaya, F. Gama, J. Paulos, G. Pappas, V. Kumar, and A. Ribeiro. Learning decentralized controllers for robot swarms with graph neural networks. In *Conf. Robot Learn.*, pp. 671–682, 2020.

Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and S. Yu Philip. A comprehensive survey on graph neural networks. *IEEE Trans. Neural Netw. Learn. Syst.*, 2020.

L. Zhang, G. Wang, and G. B. Giannakis. Real-time power system state estimation and forecasting via deep unrolled neural networks. *IEEE Trans. on Signal Process.*, 67(15):4069–4077, 2019.

F. Zhou, Q. Yang, T. Zhong, D. Chen, and N. Zhang. Variational graph neural networks for road traffic prediction in intelligent transportation systems. *IEEE Trans. Ind. Inf.*, pp. 2802–2812, 2020.

J. Zhou, G. Cui, Z. Zhang, C. Yang, Z. Liu, L. Wang, C. Li, and M. Sun. Graph neural networks: A review of methods and applications. *arXiv:1812.08434*, 2018.

R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas. MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Trans. Power syst.*, 26:12–19, 2010.

D. Zügner, O. Borchert, A. Akbarnejad, and S. Guennemann. Adversarial attacks on graph neural networks: Perturbations and their patterns. *ACM Trans. Knwl. Discov. from Data*, 14:1–31, 2020.
A Appendix—Graph Neural Networks

GNNs are parametric models to represent functional relationship for graph structured data. Specifically, the input to a GNN is a data matrix $X$. Upon multiplying the input $X$ by $W$, features will diffuse over the graph, giving a new graph signal $\mathbf{Y} = WX$. To model feature propagation, one can also replace $W$ with the (normalized) graph Laplacian or random walk Laplacian, since they will also preserve dependencies among nodal attributes.

During the diffusion process, the feature vector of each node is updated by a linear combination of its neighbors. Take the $n$-th node as an example, the shifted $f$-th feature $[\mathbf{Y}]_{nf}$ is obtained by

$$
[\mathbf{Y}]_{nf} = \sum_{i=1}^{N_n} [W]_{ni} [X]_{if} = \sum_{i \in N_n} w_{ni} x_i^f,
$$

where $N_n$ denotes the set of neighboring nodes for node $n$. The so-called convolution operation in GNNs utilizes topology to combine features, namely

$$
\mathbf{Y}^{ld} := \left[ H \ast \mathbf{X}^{l-1} ; \mathbf{W}^{ld} \right] := K_{l-1} \sum_{k=0}^{K_{l-1}} [W^k \mathbf{X}^{l-1}]_n [H^l]_d
$$

where $H := \begin{bmatrix} H_0 & \cdots & H_{K-1} \end{bmatrix}$ with $H_k \in \mathbb{R}^{F \times D}$ as filter coefficients; $\mathbf{Y} \in \mathbb{R}^{N \times D}$ the intermediate (hidden) matrix with $D$ features per node; and $W^k \mathbf{X}$ as the linearly combined features of nodes within the $k$-hop neighborhood.

To construct a GNN with $L$ hidden layers, first let us denote by $X_{l-1}$ the output of the $(l-1)$-th layer, which is also the $l$-th layer input for $l = 1, \ldots, L$, and $X_0 = X$ to represent the input matrix. The hidden $Y_l \in \mathbb{R}^{N \times D_l}$ with $D_l$ features is obtained by applying the graph convolution operation $\mathbf{H}$ at layer $l$, i.e., $[Y]_{nd} = \sum_{k=0}^{K_l-1} [W^k \mathbf{X}^{l-1}]_n [H^l]_{dk}$, where $H^l \in \mathbb{R}^{F_l \times F_l}$ is the convolution coefficients for $k = 0, \ldots, K_l - 1$. The output at layer $l$ is constructed by applying a graph convolution followed by a point-wise nonlinear operation $\sigma_l(\cdot)$. The input-output relationship at layer $l$ can be represented succinctly by $X_l = \sigma_l(Y_l) = \sigma_l(\sum_{k=0}^{K_l-1} W^k \mathbf{X}^{l-1} H^l_k)$. Using this mapping, GNNs use a nested architecture to represent nonlinear functional operator $X_L = f(X_0; \theta, W)$ that maps the GNN input $X_0$ to label estimates by taking into account the graph structure through $W$. Specifically, in a compact representation we have that

$$
f(X_0; \theta, W) := \sigma_L \left( \sum_{k=0}^{K_l} W^k \left( \cdots \left( \sigma_1 \left( \sum_{k=0}^{K_1-1} W^k X^{l-1} H^l_k \right) \cdots \right) \right) H^l_k \right)
$$

where the parameter set $\theta$ contains all the trainable filter weights $\{H^l_k, \forall l, k\}$.