CF-GNNExplainer: Counterfactual Explanations for Graph Neural Networks

Ana Lucic  
University of Amsterdam  
Amsterdam, Netherlands  
a.lucic@uva.nl

Maartje ter Hoeve  
University of Amsterdam  
Amsterdam, Netherlands  
m.a.terhoeve@uva.nl

Gabriele Tolomei  
Sapienza University of Rome  
Rome, Italy  
gabriele.tolomei@uniroma1.it

Maarten de Rijke  
University of Amsterdam  
Amsterdam, Netherlands  
derijke@uva.nl

Fabrizio Silvestri  
Sapienza University of Rome  
Rome, Italy  
fsilvestri@diag.uniroma1.it

ABSTRACT

Given the increasing promise of Graph Neural Networks (GNNs) in real-world applications, several methods have been developed for explaining their predictions. So far, these methods have primarily focused on generating subgraphs that are especially relevant for a particular prediction. However, such methods do not provide a clear opportunity for recourse: given a prediction, we want to understand how the prediction can be changed in order to achieve a more desirable outcome. In this work, we propose a method for generating counterfactual (CF) explanations for GNNs: the minimal perturbation to the input (graph) data such that the prediction changes. Using only edge deletions, we find that our method can generate CF explanations for the majority of instances across three widely used datasets for GNN explanations, while removing less than 3 edges on average, with at least 94% accuracy. This indicates that our method primarily removes edges that are crucial for the original predictions, resulting in minimal CF explanations.

1 INTRODUCTION

Advances in machine learning (ML) have led to breakthroughs in several areas of science and engineering, ranging from computer vision, to natural language processing, to conversational assistants. Parallel to the increased performance of ML systems, there is an increasing call for the “understandability” of ML models [7]. Understanding why an ML model returns a certain outcome in response to a given input is important for a variety of reasons such as model debugging, aiding decision-making, or fulfilling legal requirements [5]. Having certified methods for interpreting ML predictions will help enable their use across a variety of applications [18].

Explainable AI (XAI) refers to the set of techniques “focused on exposing complex AI models to humans in a systematic and interpretable manner” [21]. A large body of work on XAI has emerged in recent years [2, 8]. Counterfactual (CF) explanations are used to explain predictions of individual instances in the form: “If X had been different, Y would not have occurred” [25]. CF explanations are based on CF examples: modified versions of the input sample that result in an alternative output response (i.e., prediction). If the modifications recommended are also clearly actionable, this is referred to as achieving recourse [12, 28].

To motivate our problem, we consider an ML application for computational biology. Drug discovery is a task that involves generating new molecules that can be used for medicinal purposes [26, 33]. Given a candidate molecule, a GNN can predict if this molecule has a certain property that would make it effective in treating a particular disease [9, 19, 32]. If the GNN predicts it does not have this desirable property, CF explanations can help identify the minimal change one should make to this molecule, such that it has this desirable property. This could help us not only generate a new molecule with the desired property, but also understand what structures contribute to a molecule having this property.

Although GNNs have shown state-of-the-art results on tasks involving graph data [3, 38], existing methods for explaining the predictions of GNNs have primarily focused on generating subgraphs that are relevant for a particular prediction [1, 4, 14, 16, 20, 22, 30, 34, 36, 37]. However, none of these methods are able to identify the minimal subgraph automatically since they all require the user to specify in advance the size of the subgraph, S. We show that even if we adapt existing methods to the CF explanation problem, and try varying values for S, such methods are not able to produce valid, accurate explanations, and are therefore not well-suited to solve the CF explanation problem. To address this gap, we propose CF-GNNExplainer, which generates CF explanations for GNNs.

Similar to other CF methods proposed in the literature [12, 29], CF-GNNExplainer works by perturbing data at the instance-level. In this work, the instances are nodes in the graph since we focus on node classification. In particular, our method iteratively removes edges from the original adjacency matrix based on matrix sparsification techniques, keeping track of the perturbations that lead to a change in prediction, and returning the perturbation with the smallest change w.r.t. the number of edges. We evaluate CF-GNNExplainer on three public datasets for GNN explanations and measure its effectiveness using four metrics: fidelity, explanation size, sparsity, and accuracy. CF-GNNExplainer is able to generate CF examples with at least 94% accuracy, while removing fewer than three edges on average. In this work, we (i) formalize the problem of generating CF explanations for GNNs, and (ii) propose a novel method for generating CF explanations for GNNs.
2 PROBLEM FORMULATION

Let \( f(A; X; W) \) be any GNN, where \( A \) is the adjacency matrix, \( X \) is the feature matrix, and \( W \) is the learned weight matrix of \( f \) (i.e., \( A \) and \( X \) are the inputs of \( f \), and \( f \) is parameterized by \( W \)). We define the subgraph neighbourhood of a node \( v \) as a tuple of the nodes and edges relevant for the computation of \( f(v) \) (i.e., those in the \( k \)-hop neighbourhood of \( v \)): \( G_k = (A_k, X_k) \), where \( A_k \) is the subgraph adjacency matrix and \( X_k \) is the node feature matrix for nodes that are at most \( k \) hops away from \( v \). We define a node \( v \) as a tuple of the form \( v = (A_v, x) \), where \( x \) is the feature vector for \( v \).

In general, a CF example \( x \) for an instance \( x \) according to a trained classifier \( f \) is found by perturbing the features of \( x \) such that \( f(x) \neq f(\hat{x}) \) \cite{31}. An optimal CF example \( x^* \) is one that minimizes the distance between the original instance and the CF example, according to some distance function \( d \). The resulting optimal CF explanation is \( A_v^* = x^* - x \) \cite{15}.

For graph data, it may not be enough to simply perturb node features, especially since they are not always available. This is why we are interested in generating CF examples by perturbing the graph structure instead. In other words, we want to change the features, especially since they are not always available. This is why we want to change the relationships between instances, rather than change the instances themselves. Therefore, a CF example for graph data has the form \( \bar{v} = (A_v, x) \), where \( x \) is the feature vector and \( A_v \) is a perturbed version of \( A_v \). \( A_v \) is obtained by removing some edges from \( A_v \), such that \( f(\bar{v}) \neq f(v) \).

Following Wachter et al. \cite{31} and Lucic et al. \cite{15}, we generate CF examples by minimizing a loss function of the form:

\[
\mathcal{L} = \mathcal{L}_{\text{pred}}(v, \bar{v}) + \beta \mathcal{L}_{\text{dist}}(v, \bar{v}),
\]

where \( v \) is the original node, \( f \) is the original model, \( g \) is the CF model that generates \( \bar{v} \), and \( \mathcal{L}_{\text{pred}} \) is a prediction loss that encourages \( f(\bar{v}) \neq f(v) \). \( \mathcal{L}_{\text{dist}} \) is a distance loss that encourages \( \bar{v} \) to be close to \( v \), and \( \beta \) controls how important \( \mathcal{L}_{\text{dist}} \) is compared to \( \mathcal{L}_{\text{pred}} \). The goal is to find \( \bar{v}^* \) that minimizes Equation 1: this is the optimal CF example for \( v \).

3 METHOD

Here we propose CF-GNNExplainer, a method for generating CF explanations of the form \( \bar{v} = (A_v, x) \), given a node \( v = (A_v, x) \). Our method can operate on any GNN model \( f \). To illustrate our method and avoid cluttered notation, let \( f \) be a standard, one-layer Graph Convolutional Network \cite{13} for node classification:

\[
f(A, X; W) = \text{softmax} \left[ \hat{D}^{-1/2} \hat{A} \hat{D}^{-1/2} X W \right],
\]

where \( \hat{A} = A + I \), \( I \) is the identity matrix, \( \hat{D}_{ii} = \sum_j \hat{A}_{ij} \) are entries in the degree matrix \( \hat{D} \), \( X \) is the node feature matrix, and \( W \) is the weight matrix \cite{13}.

3.1 Adjacency Matrix Perturbation

First, we define \( \tilde{A}_v = P \circ A_v \), where \( P \) is a binary perturbation matrix that sparsifies \( A_v \). Our aim is to find \( P \) for a given node \( v \) such that \( f(A_v, x) \neq f(P \circ A_v, x) \). To find \( P \), we build upon the method by Srinivas et al. \cite{24} for training sparse neural networks, where the objective is to zero out weights in \( W \). In contrast, our objective is to zero out entries in the adjacency matrix (i.e., remove edges). That is, we want to find \( P \) that minimally perturbs \( A_v \), and use it to compute \( \tilde{A}_v = P \circ A_v \). If an element \( P_{ij} = 0 \), this results in the deletion of the edges between node \( i \) and \( j \). When \( P \) is a matrix of ones, this indicates that all edges in \( A_v \) are used in the forward pass. Similar to Srinivas et al. \cite{24}, we first generate an intermediate, real-valued matrix \( \hat{P} \) with entries in \([0, 1]\), apply a sigmoid transformation, then threshold the entries to arrive at a binary \( P \); entries above 0.5 become 1, while those below 0.5 become 0. In the case of undirected graphs (i.e., those with symmetric adjacency matrices), instead of generating \( \hat{P} \) directly, we first generate a perturbation vector which we then use to populate \( \hat{P} \) in a symmetric manner.

3.2 Counterfactual Generating Model

We want our perturbation matrix \( P \) to only act on \( A_v \), not \( A_v \), in order to preserve self-loops in the message passing of \( f \) (i.e., we always want a node representation update to include the node’s representation from the previous layer). Therefore, we first rewrite Equation 2 for our illustrative one-layer case to isolate \( A_v \):

\[
f(A_v, X_v; W) = \text{softmax} \left[ (D_o + I)^{-1/2} (A_v + I)(D_o + I)^{-1/2} X_v W \right]
\]

(3)

To generate CFs, we propose a new function \( g \), which is based on \( f \), but it is parameterized by \( P \) instead of by \( W \). We update the degree matrix \( D_o \) based on \( P \circ A_v \), add the identity matrix to account for self-loops (as in \( D_o \) in Equation 2), and call this \( D_o \):

\[
(A_v, X_v, W; P) = \text{softmax} \left[ D_o^{-1/2} (P \circ A_v + I) D_o^{-1/2} X_v W \right]
\]

(4)

In other words, \( f \) learns the weight matrix while holding the data constant, while \( g \) is optimized to find a perturbation matrix that is then used to generate new data points (i.e., CF examples) while holding the weight matrix (i.e., model) constant. Another distinction between \( f \) and \( g \) is that the aim of \( f \) is to find the optimal set of weights that generalizes well on an unseen test set, while the objective of \( g \) is to generate an optimal CF example, given a particular node (i.e., \( \tilde{v} \) is the output of \( g \)).

3.3 Loss Function Optimization

We generate \( P \) by minimizing Equation 1. We adopt the negative log-likelihood (NLL) loss for \( \mathcal{L}_{\text{pred}} \):

\[
\mathcal{L}_{\text{pred}}(v, \bar{v}|f, g) = - \frac{1}{2} \left[ f(\bar{v}) = f(v) \right] \cdot \mathcal{L}_{\text{NLL}}(f(\bar{v}), g(\bar{v}))
\]

(5)

Since we do not want \( f(\bar{v}) \) to match \( f(v) \), we put a negative sign in front of \( \mathcal{L}_{\text{pred}} \), and include an indicator function to ensure the loss is active as long as \( f(\bar{v}) \neq f(v) \). Note that \( f \) and \( g \) have the same weight matrix \( W \), the main difference is that \( g \) also includes the perturbation matrix \( P \). For \( \mathcal{L}_{\text{dist}} \), we take \( d \) to be the element-wise difference between \( v \) and \( \bar{v} \). Since we do not perturb the feature values, this corresponds to the difference between \( A_v \) and \( A_{\bar{v}} \), i.e., the number of edges removed. For undirected graphs, we divide this value by 2 to account for the symmetry in the adjacency matrices. When updating \( P \), we take the gradient of Equation 1 with respect to the intermediate \( \bar{P} \), not the binary \( P \).

3.4 CF-GNNExplainer

We call our method CF-GNNExplainer and summarize its details in Algorithm 1: given an instance in the test set \( v \), we first obtain its original prediction from \( f \) and initialize \( \hat{P} \) as a matrix of ones,
Algorithm 1 CF-GNNExplainer: given a node \( v = (A_0, x) \) where \( f(v) = y \), generate the minimal perturbation, \( \tilde{v} = (A_0, x) \), such that \( f(\tilde{v}) \neq y \).

**Input:** node \( v = (x, A_0) \), trained GNN model \( f \), CF model \( g \), loss function \( L \), learning rate \( \alpha \), trade-off parameter \( \beta \), number of iterations \( K \), distance function \( d \).

\[
f(v) = y \quad \text{# Get GNN prediction}
\]

\[
P = \text{threshold}(\sigma(\bar{P}))
\]

\[
\bar{A}_0 = P \odot A_0 \\
\tilde{g}^{(k)} = \text{CF-GNNExplainer}(\bar{A}_0, x)
\]

\[
\text{if } f(v) \neq \tilde{g}^{(k)} \text{ then } \\
\tilde{\gamma}^{(k)} = \hat{g}^{(k)}
\]

\[
\text{if } L_{\text{dist}}(v, \tilde{\gamma}^{(k)}) \leq L_{\text{dist}}(v, \hat{g}^{(k)}) \text{ then } \\
\tilde{\gamma}^* = \tilde{\gamma}^{(k)} \quad \text{# Keep track of best CF}
\]

\[
\text{end if}
\]

\[
\text{return } \tilde{\gamma}^*
\]

\( J_n \), to initially retain all edges. Next, we run CF-GNNExplainer for \( K \) iterations. To find a CF example, we use Equation 4. First, we compute \( P \) by thresholding \( \bar{P} \) (see Section 3.1). Then we use \( P \) to obtain the sparsified adjacency matrix that gives us a candidate CF example. This example is then fed to the original GNN, \( f \), and if \( f \) predicts a different output than for the original node, we have found a valid CF example, \( \tilde{v} \). We keep track of the “best” CF example (i.e., the most minimal according to \( d \)), and return this as the optimal CF example \( \tilde{\gamma}^* \) after \( K \) iterations. Between iterations, we compute the loss following Equations 1 and 5, and update \( \bar{P} \) based on the gradient of the loss. In the end, we retrieve the optimal CF explanation \( \Delta^*_\gamma = \bar{v} - \tilde{\gamma}^* \).

4 EXPERIMENTAL SETUP

We use the tree-cycles, tree-grids, ba-shapes node classification datasets from Ying et al. [34] to run our experiments for generating CF examples. These datasets were created specifically for the task of explaining predictions from GNNs. Each dataset consists of (i) a base graph, (ii) motifs that are attached to random nodes of the base graph, and (iii) additional edges that are randomly added to the overall graph. They are all undirected graphs. The classification task is to determine whether or not the nodes are part of the motif. The purpose of these datasets is to have a ground-truth for the “correctness” of an explanation: for nodes in the motifs, the explanation is the motif itself [17]. tree-cycles consists of a binary tree base graph with cycle-shaped motifs, tree-grids also has a binary tree as its base graph, with 3×3 grids as the motifs. For ba-shapes, the base graph is a Barabasi-Albert (BA) with house-shaped motifs, where each motif consists of 5 nodes. Here there are 4 possible classes: top of house, middle of house, bottom of house, or not part of the house. We use the same dataset splits (80% train, 10% validation, 10% test) and training setup as Ying et al. to train a 3-layer GCN (hidden size = 20) for each node classification task. Our GCNs have at least 87% accuracy on the test set.

To evaluate our method, we compare against 4 baselines: random, only-1hop, rm-1hop, and GNNExplainer. The random perturbation is meant as a sanity check. We randomly initialize the entries of \( \tilde{P} \in [-1, 1] \) and apply the same sigmoid transformation and thresholding as described in Section 3.1. We repeat this \( K \) times and keep track of the most minimal perturbation resulting in a CF example. Next, we compare against baselines that are based on the 1-hop neighbourhood of \( v \) (i.e., its ego graph): only-1hop keeps all edges in the ego graph of \( v \), while rm-1hop removes all edges in the ego graph of \( v \).

Our fourth baseline is based on GNNExplainer by Ying et al. [34], which identifies the S most relevant edges for the prediction (i.e., the most relevant subgraph of size S). To generate CF explanations, we remove the subgraph generated by GNNExplainer. We include this method in our experiments in order to have a baseline based on a prominent GNN XAI method, but we note that such subgraph-retrieving methods are not meant for generating CF explanations. Unlike our method, GNNExplainer cannot automatically find a minimal subgraph and therefore requires the user to determine the number of edges to keep in advance (i.e., the value of S). As a result, we cannot evaluate how “minimal” its CF explanations are, but we can compare it against our method in terms of its ability to generate valid CF examples (Fidelity) and how accurate those CF examples are (Accuracy). We perform a hyperparameter search over S and choose the setting that produces the most CF examples. Data and code for all experiments is available at https://github.com/a-lucic/cf-gnnexplainer.

5 RESULTS

We evaluate these CF examples in terms of four metrics: (i) Fidelity, (ii) Explanation Size, (iii) Sparsity, and (iv) Accuracy. The results are shown in Table 1. In almost all settings, we find that CF-GNNExplainer outperforms the baselines in terms of Explanation Size, Subgraph Impact, and Accuracy, which shows that CF-GNNExplainer satisfies our objective of accurately finding minimal CF examples. In cases where the baselines outperform our method on a particular metric, these baselines either perform poorly on the rest of the metrics, or on other datasets.

5.1 Fidelity

Fidelity is defined as the proportion of nodes where the original predictions match the prediction for the explanations [36]. Since we generate CF examples, we do not want the original prediction to match the prediction for the explanation, so we want a low value for Fidelity. CF-GNNExplainer outperforms only-1hop and GNNExplainer across all three datasets, and outperforms rm-1hop...
5.2 Explanation Size

Explanation Size is the number of removed edges. It corresponds to the $L_{dist}$ term in Equation 1: the difference between the original $A_v$ and the counterfactual $\bar{A}_v$. Since we want to have minimal explanations, we want a small value for this metric. Figures 1 to 5 show histograms of the Explanation Size for the five methods we test. We see that across all three datasets, CF-GNNExplainer has the smallest (i.e., most minimal) Explanation Sizes. This is especially true when comparing to random and only-1hop for the BA-shapes dataset, where we had to use a different scale for the x-axis due to how different the Explanation Sizes were. We postulate that this difference could be because BA-shapes is a much more densely connected graph; it has fewer nodes but more edges compared to the other two datasets, and the average number of nodes and edges in the subgraph neighbourhood is order(s) of magnitude larger. Therefore, when performing random perturbations, there is substantial opportunity to remove edges that do not necessarily need to be removed, leading to much larger Explanation Sizes. When there are many edges in the subgraph neighbourhood, removing everything except the 1-hop neighbourhood, as is done in only-1hop, also results in large Explanation Sizes. In contrast, the loss function used by CF-GNNExplainer ensures that only a few edges are removed, which is the desirable behavior since we want minimal explanations.

5.3 Sparsity

Sparsity measures the proportion of edges in $A_v$ that are removed [36]. A value of 0 indicates all edges in $A_v$ were removed. Since we want minimal explanations, we want a value close to 1. CF-GNNExplainer outperforms all four baselines for all three datasets in terms of Sparsity. We note CF-GNNExplainer and RM-1hop perform much better on this metric in comparison to the other methods, which aligns with the results from Explanation Size.

5.4 Accuracy

Accuracy is the proportion of explanations that are “correct”. Following Ying et al. [34] and Luo et al. [17], we only compute accuracy for nodes that are originally predicted as being part of the motifs, since accuracy can only be computed on instances for which we know the ground truth explanations. Since we want minimal explanations, we consider an explanation to be correct if it exclusively involves edges that are inside the motifs (i.e., only removes edges that are within the motifs). We observe that our method has the highest Accuracy for the tree-cycles and tree-grid datasets, whereas RM-1hop has the highest Accuracy for BA-shapes. However, we are unable to calculate the accuracy of RM-1hop for the other two datasets since it is unable to generate any CF examples for the motif nodes, contributing to the undesirable high Fidelity on those datasets. We observe Accuracy levels upwards of 94% for our method across all datasets, indicating that it is consistent in correctly removing edges that are crucial for the initial predictions.

5.5 Summary of Results

Evaluating on four distinct metrics for each dataset gives us a more holistic view of the results. We find that for all three datasets, CF-GNNExplainer can generate CF examples for the majority of nodes in the test set, while only removing a small number of edges. For nodes where we know the ground truth (i.e., those in the motifs) we achieve at least 94% Accuracy. Although random can generate CF examples for every node, they are not very minimal or accurate. The latter is also true for only-1hop – in general, it has the worst scores for Explanation Size, Sparsity and Accuracy. GNNExplainer performs at a similar level, indicating that although it is a prominent GNN XAI method, it is not well-suited for solving the CF explanation problem. RM-1hop is competitive in terms of Explanation Size, but it performs poorly in terms of Fidelity for the tree-cycles and tree-grid datasets, and its Accuracy on these datasets is unknown since it is unable to generate any CF examples for nodes in the motifs. These results show that our method is simple and extremely effective in solving the CF explanation task, unlike existing GNN XAI methods.

6 RELATED WORK

Several GNN XAI approaches have been proposed – a recent survey of the most relevant work is presented by Yuan et al. [36]. However, unlike our work, none of the methods in this survey generate CF explanations. The vast majority of GNN explanation methods are based on retrieving a relevant subgraph of the original graph [1, 4, 14, 16, 20, 22, 30, 34, 37]. Other methods identify important node features [10] or similar examples [6]. Kang et al. [11] generate CF examples for GNNs, but their work focuses on a
different task: link prediction. Other GNN XAI methods identify important node features [10] or similar examples [6]. Yuan et al. [35] and Schnake et al. [23] generate model-level explanations for GNNs, which differs from our work since we produce instance-level explanations. Adversarial attacks [27] are also related to CF examples, but there is a distinction in the intent: adversarial examples are meant to fool the model, while CF examples are meant to explain the prediction [15]. In the context of graph data, adversarial attack methods try to make minimal perturbations to the overall graph with the intention of degrading model performance. In contrast, we are interested in generating CF examples for individual nodes, as opposed to identifying perturbations to the overall graph.

Existing work on CF explanations for tabular, image, and text data is based on perturbing feature values to generate CF examples [12,29]. However, they are not equipped to handle graph data with relationships (i.e., edges) between data points, unlike our method.

7 CONCLUSION

We propose CF-GNNExplainer, which generates CF explanations for any GNN. Our simple and effective method is able to generate CF explanations that are (i) minimal, and (ii) accurate, in terms of removing edges that we know to be crucial for the initial predictions. We evaluate our method on three commonly used datasets for GNN explanation tasks and find that these results hold across all three datasets. For future work, we plan to conduct a user study to determine if humans find CF-GNNExplainer useful in practice.

REFERENCES

Figure 1: Histograms showing Explanation Size from RANDOM. Note the x-axis for BA-SHAPES goes up to 1500. Left: TREE-CYCLES, Middle: TREE-GRID, Right: BA-SHAPES.

Figure 2: Histograms showing Explanation Size from ONLY-1HOP. Note the x-axis for BA-SHAPES goes up to 1500. Left: TREE-CYCLES, Middle: TREE-GRID, Right: BA-SHAPES.

Figure 3: Histograms showing Explanation Size from RM-1HOP. Note the x-axis for BA-SHAPES goes up to 70. Left: TREE-CYCLES, Middle: TREE-GRID, Right: BA-SHAPES.

Figure 4: Histograms showing Explanation Size from GNNEXPLAINER. Note that the y-axis goes up to 1. Left: TREE-CYCLES, Middle: TREE-GRID, Right: BA-SHAPES.

Figure 5: Histograms showing Explanation Size from our method, CF-GNNEXPLAINER. Note the x-axis for BA-SHAPES goes up to 70. Left: TREE-CYCLES, Middle: TREE-GRID, Right: BA-SHAPES.