華中科技大學

图神经网络课程报告

专　　业：　　计算机

班　　级：　　CS2002

学　　号：　　I201920024

姓　　名：　　木林

电　　话：　　15623029026

邮　　箱：　　792967028@qq.com

独创性声明

本人郑重声明本报告内容，是由作者本人独立完成的。有关观点、方法、数据和文献等的引用已在文中指出。除文中已注明引用的内容外，本报告不包含任何其他个人或集体已经公开发表的作品成果，不存在剽窃、抄袭行为。

特此声明！

作者签名： 

日期：2022 年 11 月 10 日

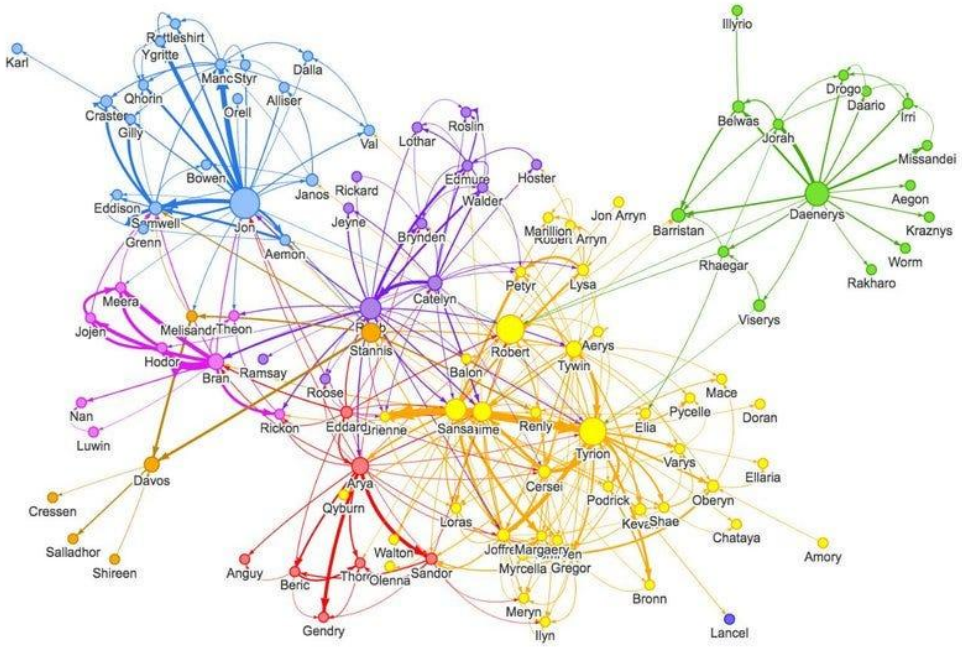
成　　绩	
教师签名	

目 录

1 概述

图形无处不在；现实世界中的对象通常是根据它们与其他事物的联系来定义的。一组对象及其之间的联系自然地表示为图形。研究人员已经开发了能够处理图形数据（称为图形神经网络或 GNN）的神经网络超过十年。最近的发展增强了它们的功能和表现力。我们开始在许多领域看到实际应用，例如抗菌发现、物理模拟、假新闻检测、交通预测等等。

本文将作为一个学习报告，希望从图形神经网络课程中学到的所有内容都能够回顾、探索更多并解释现代图形神经网络。为了简单和易于组织，我们将这项工作分为八个课程，按照课程期间每周学到的内容顺序排列，图论基础，神经网络，图嵌入，图神经网络，图神经网络的鲁棒性，图神经网络的可扩展性，图神经网络的应用，和图神经网络与大语言模型.



2 图论基础

2.1 拉普拉斯矩阵

拉普拉斯矩阵是广泛用于图论、电气网络和随机游走的图形矩阵表示。它是一种对称矩阵，用于衡量图形与其邻居之间的差异程度。拉普拉斯矩阵可以被视为图形上的负离散拉普拉斯算子的矩阵形式，近似于通过有限差分法获得的负连续拉普拉斯算子。拉普拉斯矩阵与图形的许多有用属性相关。与基尔霍夫定理一起，它可以用于计算给定图形的生成树数量。通过 Cheeger 不等式，可以通过 Fiedler 向量（对应于图形拉普拉斯的第二小特征值的特征向量）来近似图形的最稀疏切割。拉普拉斯矩阵的谱分解允许构造出在许多机器学习应用中出现的低维嵌入，并确定图形绘制中的谱布局。基于图形的信号处理基于图形傅里叶变换，它通过用与信号对应的图形拉普拉斯矩阵的特征向量替换复正弦函数的标准基础来扩展传统的离散傅里叶变换。

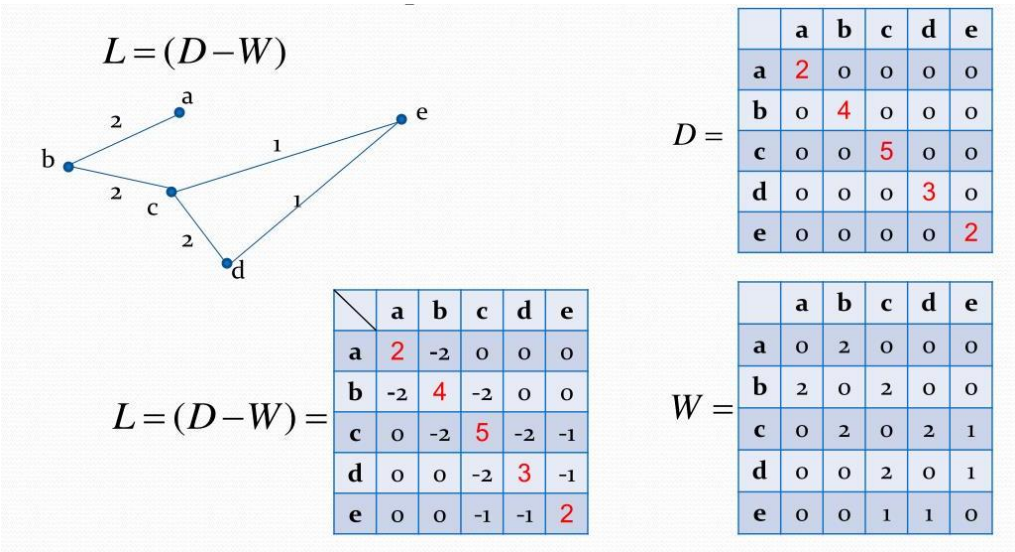


图 2.1 拉普拉斯矩阵

2.2 傅立叶变换、图傅立叶变换

图形傅里叶变换（Graph Fourier Transform，GFT）是一种数学变换，将图的拉普拉斯矩阵分解为特征值和特征向量。特征值表示频率，特征向量形成所谓的图形傅里叶基。GFT 在谱图理论中非常重要，并广泛应用于最近的图形结构学习算法研究中，例如广泛使用的卷积网络。

使用 GFT 的图形神经网络的一个例子是多维图形傅里叶变换神经网络（Multidimensional Graph Fourier Transformation Neural Network，GFTNN），它是一种在图形结构上运行的新型网络架构。 GFTNN 通过强大的操作（多维图形傅里叶变换，GFT）聚合场景属性。场景的时空车辆交互图形使用 GFT 转换为光谱场景表示。GFTNN 在区分能力方面表现出色，优于其他几种图形神经网络。

3 神经网络

神经网络是机器学习的一个子集，是深度学习算法的核心。它们由节点层组成，包含输入层、一个或多个隐藏层和输出层。每个节点连接到另一个节点，并具有关联的权重和阈值。如果任何单个节点的输出高于指定的阈值，则该节点被激活，将数据发送到网络的下一层。否则，不会传递任何数据到网络的下一层。

3.1 卷积神经网络（CNNs）

在本文中主要关注了前馈网络，但是有各种类型的神经网络，它们用于不同的用例和数据类型。例如，循环神经网络通常用于自然语言处理和语音识别，而卷积神经网络（ConvNets 或 CNN）更常用于分类和计算机视觉任务。在 CNN 之前，使用手动、耗时的特征提取方法来识别图像中的对象。然而，卷积神经网络现在提供了一种更可扩展的方法来进行图像分类和物体识别任务，利用线性代数的原理，特别是矩阵乘法，来识别图像中的模式。尽管如此，它们可能需要计算量大，需要图形处理单元（GPU）来训练模型。卷积神经网络通过其对图像、语音或音频信号输入的卓越性能与其他神经网络区分开来。

卷积层是卷积网络的第一层。虽然卷积层可以跟随其他卷积层或池化层，但全连接层是最后一层。随着每一层，CNN 的复杂性增加，识别图像的更大部分。早期的层专注于简单的特征，如颜色和边缘。随着图像数据通过 CNN 的层逐渐进展，它开始识别对象的更大元素或形状，直到最终识别出预期的对象。卷积层是 CNN 的核心构建块，是大多数计算发生的地方。它需要一些组件，包括输入数据、过滤器和特征映射。假设输入是彩色图像，由 3D 像素矩阵组成。这意味着输入将具有三个维度——高度、宽度和深度，对应于图像中的 RGB。我们还有一个特征检测器，也称为内核或过滤器，它将移动到图像的感受域，检查是否存在该特征。这个过程称为卷积。

特征检测器是一个二维（2-D）权重数组，表示图像的一部分。虽然它们的大小可以不同，但过滤器大小通常是 3x3 矩阵；这也确定了感受域的大小。然后将过滤器应用于图像的某个区域，并在输入像素和过滤器之间计算点积。然后将此点积馈送到输出数组中。之后，过滤器按步幅移动，重复该过程，直到核扫过整个图像。从输入和过滤器的一系列点积的最终输出称为特征映射、激活映射或卷积特征。特征检测器中的权重在其移动图像时保持不变，这也称为参数共享。一些参数，如权重值，通过反向传播和梯度下降的过程在训练期间进行调整。但是，在神经网络训练开始之前，需要设置三个影响输出体积大小的超参数。这些包括：在每次卷积操作之后，CNN 将对特征映射应用修正线性单元（ReLU）变换，引入非线性到模型中。

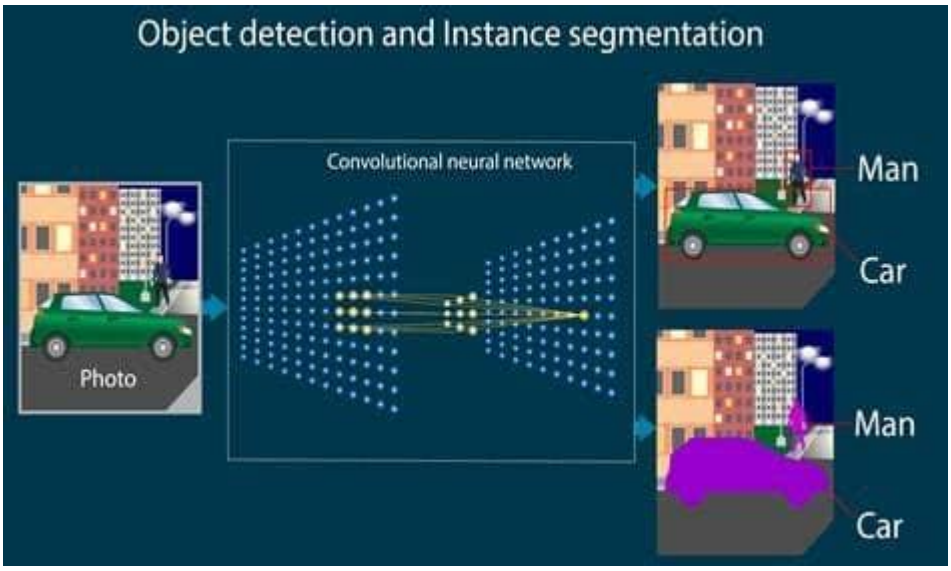


图 3.1 卷积神经网络

3.2 循环神经网络（RNNs）

循环神经网络（RNN）是一种人工神经网络类型，它使用顺序数据或时间序列数据。这些深度学习算法通常用于序数或时间问题，例如语言翻译、自然语言处理（NLP）、语音识别和图像字幕；它们被纳入流行应用程序，例如 Siri、语音搜索和 Google 翻译。与前馈和卷积神经网络（CNN）一样，循环神经网络

利用训练数据进行学习。它们通过“记忆”来区分，因为它们从先前的输入中获取信息以影响当前的输入和输出。虽然传统的深度神经网络假定输入和输出彼此独立，但循环神经网络的输出取决于序列中的先前元素。虽然未来的事件对于确定给定序列的输出也有帮助，但单向循环神经网络无法在其预测中考虑这些事件。

循环神经网络（RNN）的另一个显著特征是它们在网络的每一层之间共享参数。虽然前馈网络在每个节点上具有不同的权重，但循环神经网络在网络的每一层中共享相同的权重参数。尽管如此，这些权重仍然通过反向传播和梯度下降的过程进行调整，以促进强化学习。

循环神经网络利用时间反向传播（BPTT）算法来确定梯度，这与传统的反向传播略有不同，因为它特定于序列数据。BPTT 的原则与传统的反向传播相同，模型通过计算从其输出层到其输入层的错误来进行自我训练。这些计算允许我们适当地调整和拟合模型的参数。BPTT 与传统方法的不同之处在于，BPTT 在每个时间步骤上求和误差，而前馈网络不需要求和误差，因为它们不在每个层之间共享参数。

通过这个过程，RNN 通常会遇到两个问题，即梯度爆炸和梯度消失。这些问题由梯度的大小定义，梯度是沿着误差曲线的损失函数的斜率。当梯度太小时，它会继续变小，更新权重参数，直到它们变得微不足道，即 0。当发生这种情况时，算法不再学习。梯度爆炸发生在梯度太大时，创建不稳定的模型。在这种情况下，模型权重将变得过大，并最终表示为 NaN。解决这些问题的一种方法是减少神经网络中的隐藏层数，消除 RNN 模型中的一些复杂性。

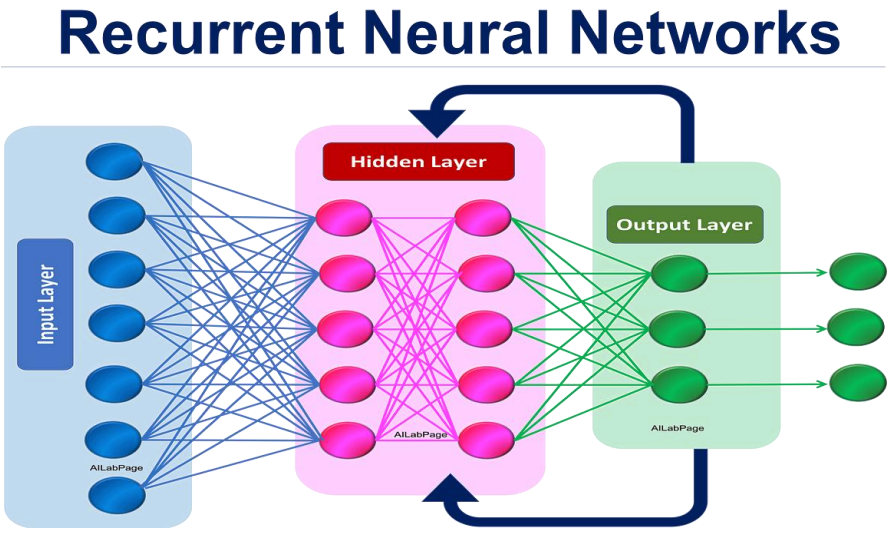


图 3.2 循环神经网络

3.3 Auto encoder

Auto encoder Graph Neural Network（GNN）是一种使用自编码器的 GNN，自编码器是一种特殊类型的神经网络，用于无监督学习。自编码器被训练为将其输入复制到其输出中。它学习两个函数：一个编码函数，用于转换输入数据，以及一个解码函数，用于从编码表示中重新创建输入数据。

在 GNN 的上下文中，自编码器可用于学习图形数据的有效表示。例如，已经为无监督的 GNN 训练提出了通过邻域 Wasserstein 重构的图形自动编码器。该模型旨在重构图形中每个节点的整个邻域信息，考虑到接近性和结构。

自编码器应用于许多问题，包括特征检测、异常检测和获取单词的含义。它们还是生成模型，可以随机生成类似于输入数据的新数据。

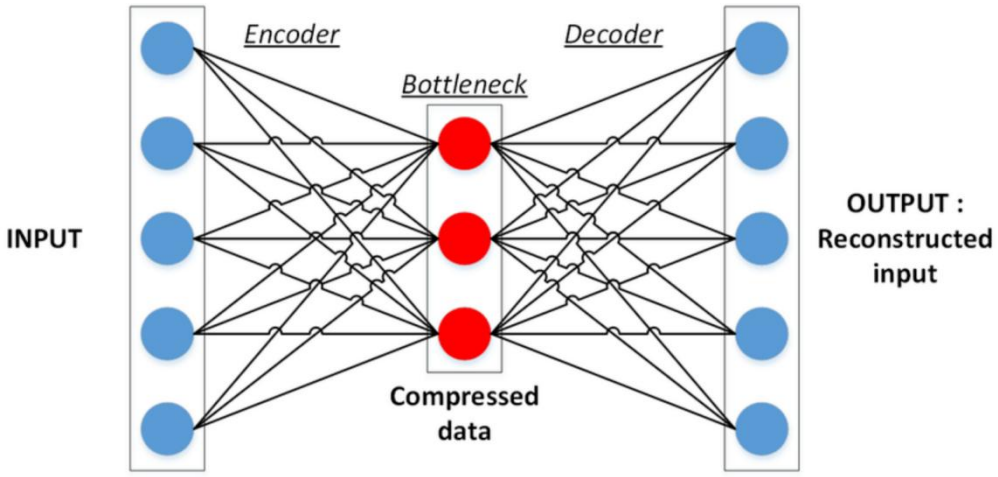


图 3. 3 Auto encoder

4 图嵌入

4.1 图嵌入法

图嵌入是一种方法，用于将节点、边缘及其特征转换为向量空间（较低维度），同时最大限度地保留图形结构和信息等属性。图形很棘手，因为它们在规模、特定性和主题方面可能会有所不同。图嵌入技术将图形嵌入到较低维度的连续潜在空间中，然后通过机器学习模型传递该表示。遍历嵌入方法执行图形遍历，目的是保留结构和特征，并聚合这些遍历，然后可以通过循环神经网络传递。接近度嵌入方法使用深度学习方法和/或接近度损失函数来优化接近度，使原始图形中彼此靠近的节点在嵌入中也是如此。其他方法使用诸如图形粗化之类的方法，在对图形应用嵌入技术之前简化图形，从而减少复杂性，同时保留结构和信息。有很多方法可以将机器学习应用于图形。其中最简单的一种是将图形转换为更易于理解的格式。

分子可以表示为小型、稀疏且静态的图形，而社交网络可以由大型、密集且动态的图形表示。最终，这使得很难找到一种银弹嵌入方法。将涵盖的方法在不同数据集上的性能各异，但它们是深度学习中最广泛使用的方法。

如果我们将嵌入视为向较低维度的转换，则嵌入方法本身不是神经网络模型的一种类型。相反，它们是一种算法类型，用于图形预处理，目的是将图形转换为计算上易于消化的格式。这是因为图形类型数据本质上是离散的。

正如最近的工作所示，有多种方法可以嵌入图形，每种方法的粒度不同。嵌入可以在节点级别、子图级别或通过图形遍历等策略上执行。这些是最流行的方法之一。

Deepwalk 不是第一种这样的方法，但它是第一种广泛用于与其他图形学习方法进行比较的方法之一。Deepwalk 属于使用步行的图形嵌入技术家族，步行

是图形理论中的一个概念，它使得可以从一个节点移动到另一个节点遍历图形，只要它们连接到公共边缘。

- DeepWalk

采用的方法是使用以下方程式完成一系列随机游走：

$$\Pr\left(v_i \mid \left(\Phi(v_1), \Phi(v_2), \cdots, \Phi(v_{i-1})\right)\right)$$

目标是估计在随机游走中到目前为止访问的所有先前节点的情况下观察节点 vi 的可能性，其中 Pr（）是概率，Φ是表示图中每个节点 v 的潜在表示的映射函数。

潜在表示是神经网络的输入。基于遇到的节点以及节点遇到的频率，神经网络可以对节点特征或分类进行预测。

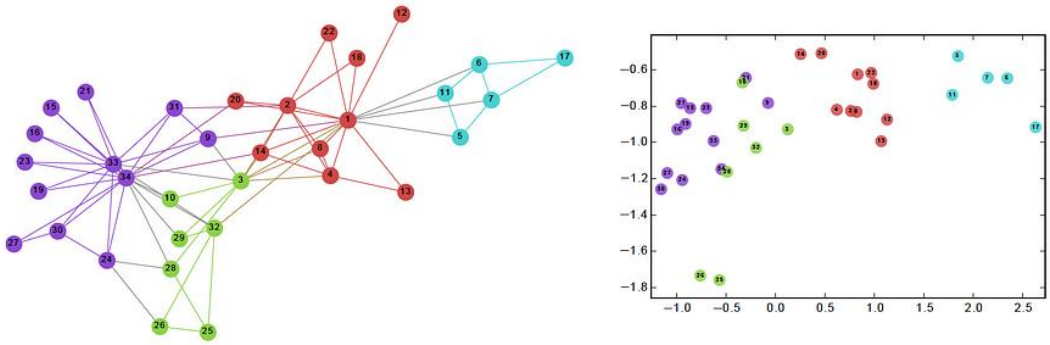


图 4. 1 DeepWalk

用于进行预测的方法是 skip-gram，就像 Word2vec 架构用于文本一样。DeepWalk 沿着图形运行以学习嵌入，而不是沿着文本语料库运行。该模型可以采用目标节点来预测其“context”，在图形的情况下，这意味着它的连通性、结构角色和节点特征。

尽管 DeepWalk 的效率相对较高，得分为 O（| V |），但这种方法是传导的，这意味着每当添加新节点时，模型必须重新训练以嵌入并从新节点中学习。

- Node2vec

Node2vec 是一种更受欢迎的图形学习方法之一，是第一批从图形结构化数据中学习的深度学习尝试之一。Node2vec 与 DeepWalk 之间的差异微妙但重要。Node2vec 具有步行偏差变量α，该变量由 p 和 q 参数化。参数 p 优先考虑广度优先搜索（BFS）过程，而参数 q 优先考虑深度优先搜索（DFS）过程。因此，下一步的决策受到概率 1 / p 或 1 / q 的影响。

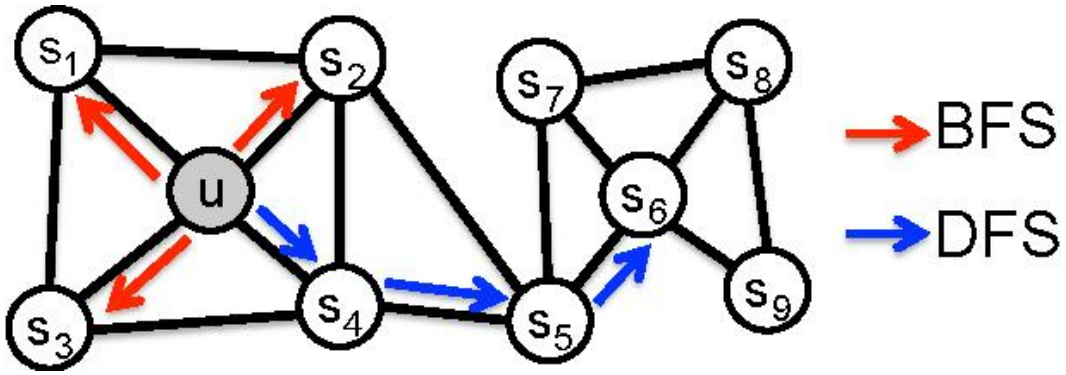


图 4. 2 Node2vec

如可视化所示，BFS 适用于学习本地邻居，而 DFS 更适合学习全局变量。Node2vec 可以根据任务在两个优先级之间切换。这意味着，给定单个图形，Node2vec 可以根据参数的值返回不同的结果。与 DeepWalk 一样，Node2vec 还采用步行的潜在嵌入，并将其用作神经网络的输入来对节点进行分类。

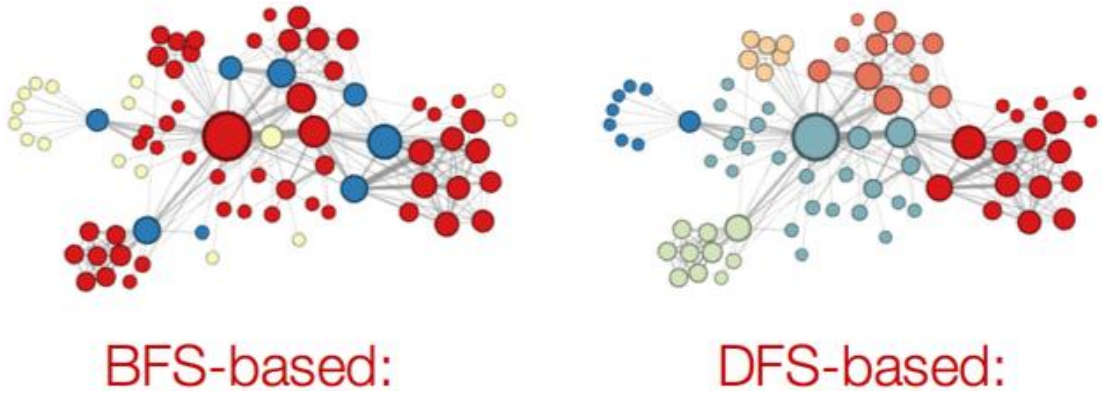


图 4.3 Node2vec

实验表明，BFS 更适合根据结构角色（中心、桥梁、离群值等）进行分类，而 DFS 返回更多基于社区的分类方案。Node2vec 是许多图形学习项目之一，它来自于斯坦福大学的 SNAP 研究小组，致力于图形分析。他们的许多作品是几何深度学习的许多重大进展的起源。

- LINE

一阶接近度的损失函数和二阶重构损失函数一起被最小化，以返回一个图嵌入。然后神经网络从嵌入中学习。 LINE 明确定义了两个函数；一个用于一阶接近度，另一个用于二阶接近度。在原始研究进行的实验中，二阶接近度的表现明显优于一阶，暗示包括更高阶可能会使精度的提高趋于平稳。 LINE 的目标是最小化输入和嵌入分布之间的差异。这是通过使用 KL 散度来实现的：

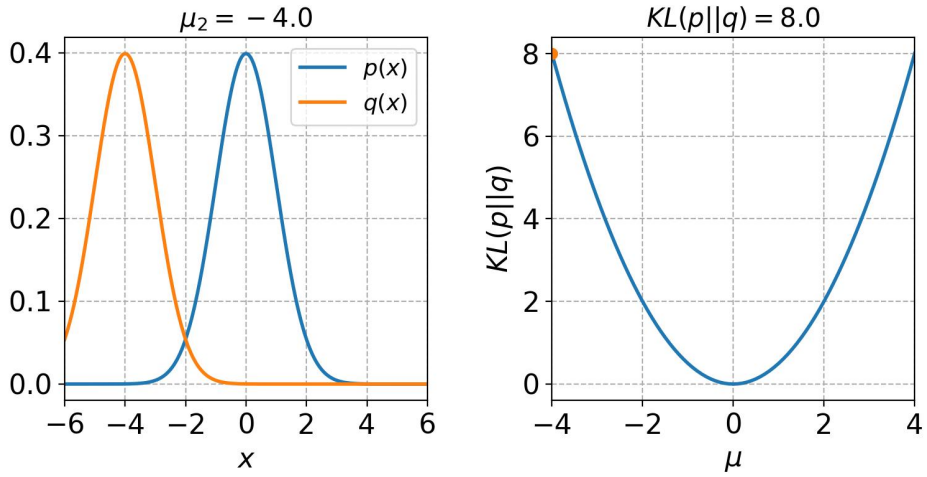


图 4. 4 LINE

LINE 为每对节点定义了两个联合概率分布，然后最小化分布的 KL 散度。这两个分布是邻接矩阵和节点嵌入的点积。KL 散度是信息理论和熵中的一个重要的相似性度量。该算法用于概率生成模型，如变分自编码器，它将自编码器的输入嵌入到一个潜在空间，这就成为了分布。 由于该算法必须为每个增加的接近度定义新的函数，所以如果应用需要理解节点社区结构，LINE 的表现并不是很好。 然而，LINE 的简单性和有效性只是它成为 2015 年 WWW 上被引用最多的论文的几个原因之一。这项工作帮助激发了对图学习作为机器学习和特别是深度学习中的一个细分领域的兴趣。

5 图神经网络

5.1 图滤波

5.1.1 ChebNet

ChebNet 是一种图神经网络（GNN），它使用切比雪夫多项式来逼近谱图卷积。它是设计谱卷积网络的早期尝试之一，也是图学习中的一个难题。然而，图卷积网络（GCN）通过只利用前两个切比雪夫多项式简化了 ChebNet，在实际数据集上的表现仍然优于它。GPR-GNN 和 BernNet 等其他模型也证明，在学习谱图卷积方面，单项式基和伯恩斯坦基优于切比雪夫基。有趣的是，这与近似理论领域的直觉相反，在近似理论中，切比雪夫多项式达到了近似函数的最佳收敛速率。ChebNet 性能较差的主要原因是 ChebNet 在逼近解析滤波函数时学习到了非法系数，从而导致过度拟合。

5.1.2 GraphSage-Filter

GraphSAGE（图形采样与聚合）是一种图形神经网络（GNN），它使用邻域采样策略为大型图形中的节点生成嵌入。它是一种可扩展的归纳法，通过对节点本地邻域的特征进行采样和聚合来生成嵌入。E-GraphSAGE 是 GraphSAGE 的扩展，它可以捕捉图的边缘特征和拓扑信息，用于物联网网络入侵检测。这是一种基于 GNN 的新型网络入侵检测系统（NIDS）。网络入侵检测系统的训练和评估数据通常以流量记录的形式表示，而流量记录自然可以用图的形式表示。E-GraphSAGE 是一种 GNN 方法，可以捕捉图的边缘特征和拓扑信息。

另一个模型是神经图协同过滤（NGCF），它通过在用户项目图结构上传播嵌入信息来利用该结构。这使得用户-项目图中的高阶连通性建模更具表现力，有效地将协作信号以明确的方式注入到嵌入过程中。

这些模型展示了 GNN 在从网络入侵检测到推荐系统等各种应用中的多功能性和潜力。

5.1.3 GAT-Filter

图形注意网络（GAT）是图形神经网络（GNN）的一种，可在图形结构数据上运行。它们利用掩蔽自注意层来解决之前基于图卷积或其近似值的方法的不足。通过堆叠节点能够关注其邻域特征的层，GAT 可以（隐含地）为邻域中的不同节点指定不同的权重，而不需要任何形式的高成本矩阵操作（如反转），也不需要预先了解图结构。

这使得 GAT 可随时应用于归纳和转导问题。GAT 模型已在多个既定的转导图和归纳图基准测试中取得或达到了最先进的结果。

5.1.4 ECC-Filter

ECC-Filter 图形神经网络指的是图形卷积神经网络中的动态边缘条件滤波器。这种方法将卷积算子从规则网格推广到任意图形，同时避免了频谱域，从而可以处理不同大小和连通性的图形。为了超越简单的扩散，滤波器权重以顶点邻域的特定边标签为条件。这种方法加上适当的图粗化选择，可以构建用于图分类的深度神经网络。

另一项研究提出了一种使 ConvGNN 的行为适应输入的新方法，该方法利用从节点特征向量动态生成的输入特定滤波器对图进行空间卷积。这种方法只需使用少量滤波器就能获得令人满意的结果。

5.1.5 GGNN-Filter

门控图序列神经网络（GGNN）是图神经网络（GNN）的一种，可在图结构数据上运行。它们使用门控传播模型来计算节点表示。递推是按固定步数展开的，并通过时间进行反向传播。然后使用输出模型对节点进行预测。GGNN 特别适

用于解决图结构数据问题。它们已被用于化学、自然语言语义学、社交网络和知识库等多个领域。与纯粹基于序列的模型（如 LSTM）相比，GGNN 在解决图结构问题时表现出良好的归纳偏差。

在滤波器方面，GGNN 和其他 GNN 一样，可以使用图卷积滤波器。这些滤波器用于在图中传播信息并更新节点表示。在包括 GGNN 在内的 GNN 中使用图卷积滤波器，可产生具有包络等差性和拓扑变化稳定性等基本特性的架构。

5.1.6 MPNN

信息传递神经网络（MPNN）是图神经网络（GNN）的一种，它将图卷积视为一个信息传递过程，在此过程中，信息沿着边从一个节点传递到另一个节点。它是一种空间图卷积网络。MPNN 是解释 GNN 的一般框架。它也被称为消息传递框架，在 2017 年的论文《量子化学的神经消息传递》（Neural Message Passing for Quantum Chemistry）中被介绍。

在一个具体的应用中，MPNN 被用来预测分子特性，特别是一种被称为血脑屏障通透性（BBBP）的分子特性。由于分子天然表示为无向图，因此 MPNN 等 GNN 被证明是预测分子特性的有用方法。

就性能而言，图变换器（GT）已成为图学习算法的新典范，在多个基准测试中都优于之前流行的 MPNN。然而，带有虚拟节点（VN）的 MPNN 是一种常用的启发式方法，但理论上却鲜为人知，其强大的功能足以任意逼近 GT 的自注意层。

5.1.7 PPNP

个性化神经预测传播（PPNP）是 Johannes Gasteiger 和 Stephan Günnemann 在论文 "Predict then Propagate： Johannes Gasteiger、Aleksandar Bojchevski 和 Stephan Günnemann 在论文 "Predict then Propagate: Graph Neural Networks meet Personalized PageRank "中提出的模型。

PPNP 模型利用图卷积网络 (GCN) 和 PageRank 之间的关系，推导出基于个性化 PageRank 的改进传播方案。利用这一传播程序构建了一个简单模型 PPNP 及其快速近似模型 APPNP。

PPNP 模型利用可调整的大型邻域进行分类，并可与任何神经网络轻松结合。在迄今为止针对 GCN 类模型所做的最深入研究中，它的表现优于最近提出的几种半监督分类方法。

5.1.8 APPNP

APPNP（神经预测的近似个性化传播）是一个利用图卷积网络（GCN）和 PageRank 之间的关系来推导基于个性化 PageRank 的改进传播方案的模型。

APPNP 模型利用可调整的大型邻域进行分类，并可与任何神经网络相结合。事实证明，它优于最近提出的几种对多个图进行半监督分类的方法。

5.2 图池化

图池化是许多图神经网络（GNN）架构的核心组成部分。它对于获得整个图的整体图级表示是不可或缺的。作为对传统卷积神经网络（CNN）的继承，大多数方法都将图池化表述为聚类分配问题，并将规则网格中局部补丁的概念扩展到图中。

5.2.1 gPool

gPool 是图形神经网络（GNN）中使用的一种图形池。图池化是许多图神经网络架构的重要组成部分，对于获得整个图的整体图级表示不可或缺。作为对传统卷积神经网络（CNNs）的继承，大多数方法都将图池化表述为聚类分配问题，将规则网格中局部斑块的概念扩展到图中。

文献的多样性源于对图进行粗化的多种可能策略，这些策略可能取决于对图结构或特定下游任务的不同假设。

最近的一项研究发现，仔细选择用于 GNN 中聚合和读出操作的池化函数，对于使 GNN 能够进行外推至关重要。不同任务的集合函数各不相同，如果没有正确的集合函数选择，GNN 就完全无法泛化到分布外数据，而可能的选择数量会随着层数的增加而呈指数增长。

5.2.2 SAGPool

SAGPool（自我注意力图池化）是一种基于自我注意力的图池化方法。它使用图卷积来计算注意力分数和节点特征，同时考虑图拓扑结构。在 SAGPool 方法中，使用图卷积的自我关注允许池方法同时考虑节点特征和图拓扑。这种方法已被证明可以提高性能，并得到广泛应用。

为确保公平比较，现有的池化方法和 SAGPool 方法使用了相同的训练程序和模型架构。实验结果表明，在基准数据集上，SAGPool 方法使用合理的参数数量就能获得卓越的图分类性能。

5.2.3 DiffPool

DiffPool 是一个可微分图池化模块，可以生成图的分层表示，并能以端到端的方式与各种图神经网络架构相结合。DiffPool 为深度图神经网络每一层的节点学习可微分的软集群分配，将节点映射到集群集合，然后形成下一层图神经网络的粗化输入。

6 图神经网络的鲁棒性

6.1 图对抗攻击

针对图神经网络（GNN）的对抗性攻击暴露了其安全漏洞，限制了其在安全关键型应用中的应用。这些攻击意味着攻击者会对图结构注入精心设计的微小扰动，以降低图神经网络分类器的性能。这一漏洞是阻碍 GNN 在实际应用中使用的一个重要问题。

然而，现有的攻击策略依赖于对所使用的 GNN 模型或所攻击的预测任务的了解。在最近的一项研究中，针对预算有限的物联网系统中基于 GNN 的入侵检测，引入了一种新颖的分层对抗攻击（HAA）生成方法，以实现水平感知的黑盒对抗攻击策略。

6.1.1 PGD 拓扑攻击

PGD（投射梯度下降）是一种可应用于图神经网络（GNN）的对抗性攻击。由于图神经网络易受攻击，因此对图神经网络的对抗性攻击一直是近期的研究课题。这些攻击可以以误导 GNN 的方式操纵图的结构和特征，从而可能导致不正确的预测或分类。就 GNN 而言，PGD 攻击涉及对图的结构或节点特征进行微小的修改，从而在某些限制条件下最大化 GNN 的损失。这些修改在原始图的背景下通常是难以察觉或微不足道的，但却会对 GNN 的性能产生重大影响。

有一些研究和模型与对 GNN 的对抗性攻击有关。这些研究调查了 GNN 的弱点，并提出了各种方法来提高其对抗恶意攻击的鲁棒性。投射梯度下降（PGD）是一种可用于图神经网络（GNN）的对抗性攻击。就 GNN 而言，PGD 攻击涉及对图的结构或节点特征进行微小修改，从而在某些限制条件下最大化 GNN 的损失。

这些修改在原始图的上下文中通常是难以察觉或微不足道的，但却能显著影响 GNN 的性能。例如，攻击者可以在图中插入对抗性扰动，这会导致设计良好的模型产生不正确的输出或具有糟糕的整体性能。

6.1.2 Nettack

Nettack 是一种针对图神经网络 (GNN) 的对抗性攻击方法。它是由 Daniel Zügner、Amir Akbarnejad 和 Stephan Günnemann 在论文 "Adversarial Attacks on Neural Networks for Graph Data "中提出的。

Nettack 方法是向图结构注入精心设计的微小扰动，以降低 GNN 分类器的性能。这一漏洞是阻碍 GNN 在实际应用中使用的一个重要问题。Nettack 方法是一种通过扰乱图结构和/或节点特征对图神经网络（GNN）进行对抗性攻击的方法。其目的是误导图神经网络对目标节点做出错误的预测或分类。该方法的工作原理如下：

首先，攻击者选择一个目标节点和所需的错误标签。攻击者还可以访问图结构、节点特征和训练好的 GNN 模型。

其次，攻击者计算每个节点和边对目标节点预测的影响。影响度基于 GNN 输出相对于图结构和节点特征的梯度。攻击者根据影响力对节点和边进行排序，并选择影响力最大的节点和边进行扰动。

第三，攻击者通过添加、删除或翻转边或特征来扰动图结构和/或节点特征。攻击者试图使扰动次数和扰动预算最小化，同时使目标节点的预测误差最大化。攻击者可以使用不同的优化策略，如贪婪算法、遗传算法或基于梯度的算法，来找到最优扰动。

Nettack 方法对各种 GNN 架构（如 GCN、GAT 和 GraphSAGE）都很有效，能以高概率和低扰动成本骗过 GNN。该方法还可扩展到同时攻击多个目标节点，或生成影响所有节点的通用扰动。

6.1.3 RL-S2V

RL-S2V 是一种针对图神经网络（GNN）的对抗性攻击方法。这是第一项利用强化学习对图数据产生对抗性扰动的研究。由于图神经网络易受攻击，因此对图神经网络的对抗性攻击一直是近期的研究课题。这些攻击会以误导 GNN 的方式操纵图的结构和特征，从而可能导致不正确的预测或分类。

RL-S2V 是一种基于强化学习的方法，它通过添加或删除边来对图数据产生对抗性扰动。它使用图神经网络作为策略网络来学习状态-行动值函数，以估算扰动给定边的奖励。奖励被定义为受害者模型对目标节点预测置信度的下降。RL-S2V 会反复选择状态-动作值最高的边，并根据观察到的奖励更新策略网络，直到攻击预算耗尽或攻击成功。

6.2 图对抗防御

Pro-GNN 是 "鲁棒图神经网络的图结构学习"（Graph Structure Learning for Robust Graph Neural Networks）的缩写。它是一个通用框架，可以从受扰动的图中联合学习结构图和鲁棒图神经网络模型。

Pro-GNN 方法旨在防御对图的恶意攻击。它利用了现实世界图的固有特性，如低秩和稀疏性，以及相邻两个节点的特征相似的趋势。对抗性攻击通常会违反这些图属性，而 Pro-GNN 则利用这些属性来抵御此类攻击。

Pro-GNN 通过从扰动图中联合学习结构图和鲁棒图神经网络模型来抵御对图的恶意攻击。它利用了现实世界图的固有特性，如低秩和稀疏性，以及相邻两个节点的特征相似的趋势。对抗性攻击往往会违反这些图的特性，而 Pro-GNN 则利用这些特性来抵御此类攻击。Pro-GNN 的核心原理是利用相似性特性来减轻对图的负面影响。具体来说，这种方法通过节点特征和图结构的相似性来修剪对抗性边缘，从而消除对抗性扰动。

总之，Pro-GNN 通过同时学习图结构和 GNN 参数，提高了在各种对抗性攻击下的整体鲁棒性。

7 图神经网络的可扩展性

可扩展性仍然是图神经网络（GNN）面临的主要挑战之一。一个节点的表示是通过递归聚合和转换其相邻节点在前几层的表示向量来计算的，这会导致感受野呈指数增长。这使得标准的随机优化技术失效。

目前的研究主要从逐点采样法、逐层采样法和子图采样法，这三种采样范式来解决这些障碍。这些方法分别基于图中的目标节点、卷积层或构建子图进行模型推理。

7.1 逐点采样法

逐点采样法是一种用于解决图形神经网络（GNN）中的可扩展性问题的方法。关键思想是对每个层的节点及其邻居的子集进行采样，以计算每次迭代时的随机梯度下降（SGD）。

图形采样，包括节点采样，通过以小比例对图中的节点采样来解决 GNN 中的内存问题。这样，GNN 可以扩展到更大的图。然而，大部分取样方法都集中在固定取样启发式，可能不会推广到不同的结构或任务。

遗憾的是，采样算法必须能够访问整个图形，这对于 GPU 内存来说往往太大。尽管存在这些挑战，节点采样仍然是有效培训 GNN 的关键技术。

7.2 逐层采样法

逐层采样是图神经网络（GNN）中用来提高训练效率的一种方法。这种方法包括在图神经网络的每一层对节点进行采样，构建子图，并计算相应的重要性概率。然后，它根据计算出的概率对固定数量的节点进行采样，并在每一层递归执行这样的程序，以构建整个计算图。

这种方法有利于提高 GNN 训练的效率和可扩展性，而精心设计的逐层采样方法无疑会提高训练过程的效率。最近，大量数据被采样并输入 GPU 进行训练。

7.3 子图采样法

子图采样法是图神经网络（GNN）中用来提高训练效率的一种方法。这种方法包括对 GNN 每一层的节点进行采样，构建子图，并计算相应的重要性概率。然后，它根据计算出的概率对固定数量的节点进行采样，并在每一层递归执行这样的程序，以构建整个计算图。

有几种方法涉及 GNN 中某种形式的子图采样或选择：

子图谱网络（SubGNN）： SubGNN 是一种子图神经网络，用于学习分离的子图表示。它提出了一种新颖的子图路由机制，可在子图的组成部分与底层图中随机抽样的锚斑块之间传播神经信息，从而获得高精度的子图表示。

度量引导（MeGuide）： MeGuide 是用于 GNN 的子图学习框架。MeGuide 采用了两个新颖的度量： 特征平滑度（FeatureSmoothness）和连接失败距离（ConnectionFailureDistance）来指导子图采样和基于迷你批次的训练。

NeuroMatch：NeuroMatch 是一种用于高效子图匹配的图神经网络 (GNN) 架构。给定一个大型目标图和一个较小的查询图，NeuroMatch 会识别目标图的邻域，该邻域包含作为子图的查询图。

8 图神经网络的应用

8.1 生物信息中的图神经网络

8.1.1 分子表示学习

分子表征学习（MRL）是建立机器学习与化学科学之间联系的关键一步。特别是，它将分子编码为保存分子结构和特征的数字向量，在此基础上执行下游任务（如性质预测）。

图神经网络（GNN）已广泛应用于分子图的特征表示学习。例如，通过图神经网络进行分子对比表征学习（MolCLR）就是一种利用大量未标记数据的自我监督学习框架。在 MolCLR 预训练中，建立了分子图，并开发了 GNN 编码器来学习可微分表征。

最近，MRL 取得了长足的进步，尤其是基于深度分子图学习的方法。本研究将系统回顾这些基于图的分子表征技术，尤其是包含化学领域知识的方法。

例如，MolCLR：通过图神经网络（GNNs）进行分子对比表征学习（Molecular Contrastive Learning of Representations via Graph Neural Networks, GNNs）是一种利用大量未标记数据的自监督学习框架。在 MolCLR 预训练中，建立了分子图，并开发了 GNN 编码器来学习可微分表征。

另一项研究表明，图神经网络（GNN）已被视为分子性质预测的一种有吸引力的建模方法，大量研究表明，与传统的基于描述符的方法相比，GNN 可以产生更有前途的结果。

然而，值得注意的是，一项比较研究发现，平均而言，基于描述符的模型在预测准确性和计算效率方面优于基于图的模型。但是，一些基于图的模型，如 Attentive FP 和 GCN，可以在部分较大或多任务数据集上产生出色的性能。

这些方法涉及某种形式的分子表征学习，可视为 GNN 中的分子表征学习。不过，具体方法取决于任务的具体要求和 GNN 的架构。

8.1.2 分子关联预测

图神经网络（GNN）已被广泛用于预测分子关联。例如，LR-GNN 是一种基于链接表示的新型 GNN，用于预测分子关联。它采用图卷积网络（GCN）编码器获得节点嵌入。为了表示分子之间的关联，设计了一种传播规则，捕捉每个 GCN 编码器层的节点嵌入来构建链接表示。所有层的链接表示通过设计的层融合规则融合输出，从而使 LR-GNN 输出更精确的结果。在四种生物医学网络数据（包括 lncRNA-疾病关联、miRNA-疾病关联、蛋白质-蛋白质相互作用和药物-药物相互作用）上的实验表明，LR-GNN 优于最先进的方法，并实现了稳健的性能。

另一个例子是 MolNet，它是一种化学直观 GNN，包含分子中的三维非键信息、非共价邻接矩阵以及来自加权键矩阵的键强度信息。对比研究表明，MolNet 的性能优于各种基线 GNN 模型，在 BACE 数据集的分类任务和 ESOL 数据集的回归任务中，MolNet 的性能达到了一流水平。

这些只是 GNN 如何用于分子关联预测的几个例子。随着新方法和新架构的不断开发，该领域正在迅速发展。

8.2 自然语言处理中的图神经网络

图神经网络（GNN）越来越多地应用于自然语言处理（NLP）领域。图神经网络提供了一种新的方法，可以沿着图构建、图表示学习和基于图的编码器-解码器模型这三个轴线系统地组织现有的 NLP 研究。

虽然由深度神经网络学习的词嵌入被广泛使用，但这些表示法无法充分利用文本片段的底层语言和语义结构。图形是捕捉不同文本片段（如实体、句子和文

档）之间联系的一种自然方式。为了克服向量空间模型的局限性，研究人员将深度学习模型与图结构表示相结合，用于 NLP 和文本挖掘中的各种任务。

这种方法有助于充分利用文本中的结构信息和深度神经网络的表征学习能力。一份调查报告全面概述了用于 NLP 的 GNN，并提出了用于 NLP 的 GNN 新分类法。这被认为是图神经网络在自然语言处理领域的首次全面概述。

8.3 代码智能中的图神经网

图形神经网络（Graph Neural Networks, GNNs）是一种强大的代码智能工具。它们可以用来分析和理解代码的结构，它自然被表示为一个图形，其中节点可以是像函数、变量、类等的各种代码元素，边表示这些元素之间的关系。GNN 可以用于多种任务，如：

- 代码完成：GNNs 可以预测代码片段中的下一个令牌,帮助开发人员更有效地编写代码。
- 错误检测：通过学习代码库的正常模式,GNN 可以将偏离这些模式的代码片段识别为潜在的错误。
- 代码摘要：GNNs 可以为代码片段生成人类可读的摘要，这对于理解大型代码库很有用。
- 代码搜索：给定自然语言查询,GNN 可以检索与查询意图相匹配的相关代码片段。
- 代码克隆检测：GNN 可以识别功能相似但文本不相同的代码片段。

但是,重要的是要注意,虽然 GNN 具有很大的前景,但它们也会带来挑战,尤其是在可扩展性和可解释性方面。尽管存在这些挑战，在代码智能中使用 GNN 是一个活跃的研究领域，并有可能显着提高开发人员的生产率和代码质量

9 图神经网络与大语言模型

图神经网络（GNN）和大语言模型（LLM）是两种强大的深度学习模型，已被广泛应用于计算机视觉、自然语言处理和知识表示等多个领域。最近，研究人员提出了几种结合 GNN 和 LLM 的方法，以充分利用它们的互补优势，在各种任务中实现更好的性能。

其中一种方法是图形神经提示（GNP），它是一种即插即用的方法，可以帮助预先训练好的 LLM 从知识图谱（KG）中学习有益的知识。GNP 包含多种设计，包括标准图神经网络编码器、跨模态池模块、域投影器和自监督链接预测目标。在多个数据集上进行的大量实验证明，在不同规模和设置的语言模型中，GNP 在常识推理和生物医学推理任务上都具有优势。

另一种方法是语言模型图神经网络（LM-GNN），它是一种联合训练大规模语言模型和图神经网络的高效框架。LM-GNN 的有效性是通过对 BERT 模型进行阶段性微调实现的，首先使用异构图信息，然后使用 GNN 模型。

这些只是 GNN 和 LLM 如何结合以在各种任务中实现更好性能的几个例子。随着新方法和新架构的不断开发，这一领域正在迅速发展。

10 课程感想

图形神经网络（Graph Neural Networks，GNNs）是处理可以表示为图形的数据的强大工具。它们通过图形节点之间的消息传递捕获图形的依赖性。修完课程后,以下是学习 GNN 的一些理由,以及 GNN 的优缺点：

学习 GNN 的原因：

- 丰富的数据表示：许多现实世界的系统自然被表示为图形，如社交网络、生物网络和万维网。GNN 提供了一种处理和学习这些结构丰富的数据的方法。
- 卓越的性能：GNNs 在许多深度学习任务上展示了突破性的性能。
- 广泛应用：GNNs 在自然语言处理、社交网络、引文网络、分子生物学、化学、物理、NP 硬组合优化问题等各个领域都有应用。

GNN 的优势：

- 图形数据处理：GNNs 可以处理包含元素间丰富关系信息的图形数据。
- 量化不确定性：GNN 的一个主要好处是能够量化图形结构深度学习中的不确定性。

GNN 的缺点：

- 可扩展性问题：GNN 中一个节点的表示是通过递归聚合和转换其来自先前层的相邻节点的表示向量来计算的,从而导致接收字段呈指数增长。这使得标准随机优化技术无效。
- 内存需求：大多数 GNN 模型通常计算图形的整个邻接矩阵和节点嵌入,这需要巨大的内存空间。

- 性能不良：当输入图数据信息薄弱,即结构不完整、特征不完整和标签不足时,GNN 的性能可能会恶化。

尽管存在这些挑战，在各种应用中使用全球导航网络是一个有趣的活跃研究领域，并更多地了解其在显着改善世界各种有用任务方面的潜力。

参考文献

[1] Zhou, J., Cui, G., Zhang, Z., Yang, C., Liu, Z., Wang, L., Li, C., & Sun, M. (2020). Graph Neural Networks: A Review of Methods and Applications. AI Open.

[2] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2019). A Comprehensive Survey on Graph Neural Networks. IEEE Transactions on Neural Networks and Learning Systems.

[3] Battaglia, P. W., Hamrick, J. B., Bapst, V., Sanchez-Gonzalez, A., Zambaldi, V., Malinowski, M., ... & others. (2018). Relational inductive biases, deep learning, and graph networks. arXiv preprint.

[4] Scarselli, F., Gori, M., Tsoi, A. C., Hagenbuchner, M., & Monfardini, G. (2009). The graph neural network model. IEEE Transactions on Neural Networks.

[5] Waikhom, L., & Patgiri, R. (2021). Graph Neural Networks: Methods, Applications, and Opportunities. arXiv preprint.

[6] Skarding, J., Gabrys, B., & Musial, K. (2020). Foundations and modelling of dynamic networks using Dynamic Graph Neural Networks: A survey. arXiv preprint.

[7] Liu, Z., & Zhou, J. (2020). Introduction to Graph Neural Networks. Synthesis Lectures on Artificial Intelligence and Machine Learning, Morgan & Claypool Publishers.

[8] Sun, L., Dou, Y., Yang, C., Wang, J., & Yu, P. S. (2018). Adversarial Attack and Defense on Graph Data: A Survey. arXiv preprint.

[9] Zhang, Z., Cui, P., & Zhu, W. (2018). Deep Learning on Graphs: A Survey. arXiv preprint.

[10] Bronstein, M. M., Bruna, J., LeCun, Y., Szlam, A., & Vandergheynst, P. (2017). Geometric Deep Learning: Going beyond Euclidean data. IEEE SPM.