

# Federated Learning on Non-IID Graphs via Structural Knowledge Sharing

Y Tan, Y Liu, G Long, J Jiang, Q Lu, C Zhang

## 摘要

本文复现了一个关于联邦研究的先进算法 FedStar<sup>[1]</sup>，这是一种联邦图学习（FGL）框架，利用图神经网络（GNNs）在分布式环境中训练强大的模型，而无需共享私人数据。在面临非独立同分布（non-IID）问题的情况下，FedStar 通过提取和共享图数据中的共同结构信息来应对挑战。通过定义结构嵌入并使用独立结构编码器对其进行编码，FedStar 能够在客户端之间共享结构信息，同时以个性化方式学习基于特征的知识。本研究着眼于 FedStar 的复现工作，并在此基础上提出了一些创新性的改进，首先介绍本研究的背景和动机，概述了需要复现的算法。随后，回顾了与该算法相关的先前研究，以及领域内的其他相关工作。接下来详细描述了复现方法，在复现细节部分，我们详细介绍了实验的具体设置、使用的数据集和算法参数等重要信息。然后，我们通过实验结果分析部分对我们的复现进行了全面的评估，在这一部分，我们讨论了实验结果，比较了我们的复现与原始研究的一致性，并提供了有关性能、效率或其他相关指标的详细分析。最后，我们总结了我们的复现工作的主要发现和结论，强调了对原始算法的复现在该领域中的重要性，和未来研究的方法。

**关键词：**联邦学习；图神经网络；联邦图学习

## 1 引言

在当今数字化时代，数据的巨大规模已经不再是我们关注的核心问题，而更加引发广泛关注的焦点在于数据的隐私和安全。法规对数据隐私的强化要求使得传统的集中式训练方法在防范数据泄露和侵犯用户隐私方面变得愈加困难。在这背景下，联邦学习作为一种创新的分布式训练方法，为解决这一难题提供了新的途径。联邦学习的关键在于赋予用户对本地数据的完全自治权，突显了对数据所有者隐私的强有力保护。传统的中心化训练方法不再是唯一选择，而是在联邦学习框架下，不同地理位置的个体用户可以协作学习机器学习模型，所有可能包含敏感个人信息的数据都可以保留在设备上。在这种环境下，用户可以从获得经过良好训练的机器学习模型中受益，而无需将隐私敏感的个人数据发送到中央服务器。

这一领域的发展为人工智能研究开辟了新的方向，特别是随着人工智能芯片的崛起，终端设备的计算资源变得更为强大。联邦学习为模型训练提供了隐私保护机制，充分利用了终端设备的计算资源，避免了在数据传输过程中私人信息泄露的风险。由于移动设备和其他领域的设备数量庞大，蕴藏了大量宝贵的数据资源，联邦学习因此能够更加充分地发挥其优势。

总体而言，联邦学习的发展在于解决隐私和安全问题上提供了一种创新性的解决方案。通过确保用户对本地数据的完全自治权，采用多层次的隐私保护机制，联邦学习不仅为人工智能研究注入新的活力，也为解决当今数字时代面临的隐私和安全挑战提供了有力支持<sup>[2]</sup>。

在联邦学习中需要解决的一些挑战，主要集中在隐私保护、数据量不足以及统计异质性等方面。

1. 首先，隐私保护是联邦学习中需要着重解决的问题之一。由于联邦学习的提出旨在解决机器学习中隐私数据保护的问题，确保在联邦学习中的训练模型不泄露用户的私人信息至关重要。这涉及采

用有效的隐私保护机制，例如加密算法、差分隐私等，以确保在联邦学习过程中用户隐私得到充分的保护。

2. 其次，数据量不足是另一个需要克服的挑战。传统的机器学习通常需要大量数据来训练出性能优越的模型，但在分布式环境下，每个移动设备上的数据量有限。同时，集中式收集所有数据可能带来巨大的成本。因此，联邦学习通过让每个设备使用本地数据进行模型训练，然后将所有本地模型上传到服务器，实现全局模型的聚合，以解决数据量不足的问题。

3. 最后，统计异质性是联邦学习中需要面对的另一个挑战。在联邦环境中存在大量边缘设备，而这些设备持有的数据可能是非独立且不同分布的（Non-IID）。例如，在智能医疗系统中，不同类型疾病的电子病历数据结构可能不同，训练这些非独立且不同分布的数据集是一个巨大的挑战。因此，联邦学习需要处理统计异质性，以适应各种边缘设备上的不同数据分布。

针对非独立同分布图（Non-IID graphs）的影响，新兴的研究分支试图缓解这一影响。这些研究采用传统的图神经网络（GNNs）作为本地编码器，并引入各种技术进行本地训练或全局聚合，例如聚类和元学习。然而，现有的联邦图学习（FGL）方法仍然通过基于特征的消息传递方案生成表示，受到来自多个领域的图的特征异质性（不同的特征空间和维度）的影响。在 FGL 过程中，对在不同特征空间上训练的 GNN 模型进行聚合可能无法捕捉在非独立同分布图上共享的有用的基础知识，从而意外地影响本地模型的个性化性能。

尽管在不同图领域中，特征信息往往是异构的，但一些底层图结构属性可以在不同领域之间共享。然而，现有的 FGL 框架难以捕捉和传递这种结构知识。首先，这些方法通常依赖于传统的 GNNs，其中结构信息被隐式编码到基于特征的节点表示中；因此，异构特征不可避免地影响结构知识学习的质量。此外，大多数 FGL 方法仍然在所有可学习参数上执行参数聚合，难以提取和共享跨客户的结构特定知识。因此，一个自然的研究问题是“在本地训练期间如何隔离异构特征中的结构信息以及如何进行联邦知识共享？”

为了回答上述问题，在这项工作中，提出了一种名为结构知识共享的联邦图学习框架（FedStar），该框架充分利用图中的自然结构信息来处理图间联邦学习任务。本文主题是捕捉并共享跨多个客户的通用结构知识，以提升 FGL 中客户端的本地性能。具体而言，首先引入了一个矢量结构嵌入，明确表示跨不同领域共享的固有结构属性。然后，为了避免特征异质性的干扰，设计了一个特征-结构解耦的 GNN，使用一个独立通道捕获高层次的结构知识，同时使用另一个通道学习属性知识。最后，设计了一个带有结构知识共享的 FL 框架，其中领域无关的结构信息在不同客户端之间共享，而基于特征的表示在本地学习。因此，客户端能够同时学习泛化的结构编码器和个性化的特征编码器。该工作的贡献有三个方面：

1. 该研究通过引入结构知识共享的新视角，针对联邦图学习中的 Non-IID 问题进行了深入研究。
2. 提出了一种创新的联邦图学习框架，名为 FedStar，该框架使客户端能够在全局学习领域不变的结构知识的同时，本地捕捉领域特定的基于特征的知识。
3. 实验证明 FedStar 在多个非独立同分布设置下一贯优于基线方法，突显了其在处理异构图数据时的有效性和优越性。

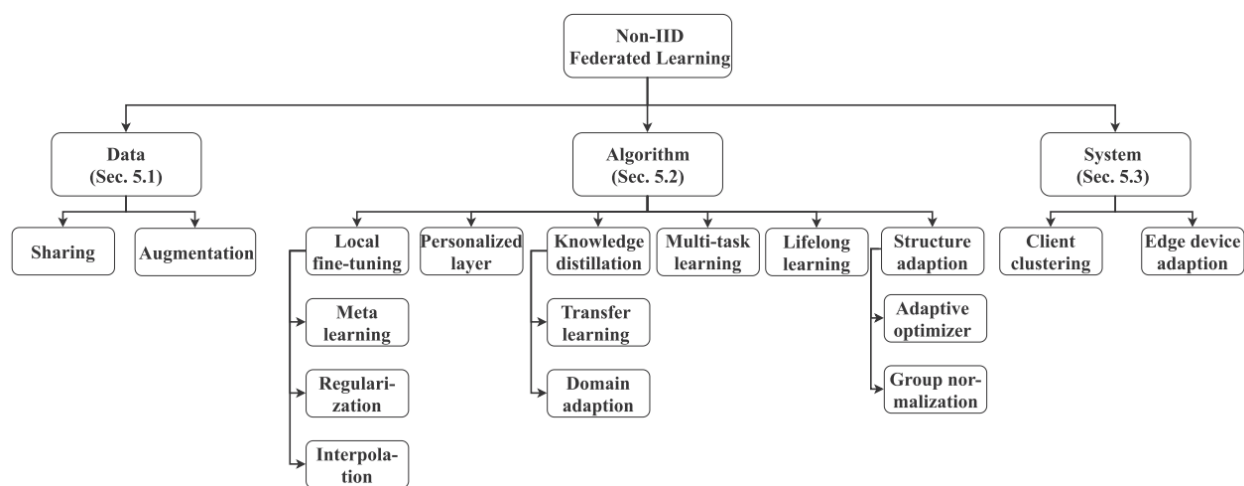


图 1: 处理非 iid 数据的现有方法

## 2 相关工作

联邦学习（Federated Learning, FL）代表了机器学习领域的一次范式转变，旨在在分布在不同设备上的数据上训练全局模型，同时优先考虑数据隐私。FL 的概念首次由 McMahan 等人于 2016 年引入，开创了一种基于数据并行性的新方法。这一方法的核心是联邦平均（Federated Averaging, FedAvg）算法<sup>[3]</sup>。作为一种分散式机器学习方法，FedAvg 使多个设备能够协同训练机器学习模型，同时确保用户数据保留在本地。这种分散式方法消除了将敏感用户数据上传到中央服务器的需求，解决了与隐私风险和数据泄露相关的担忧。相反，FedAvg 允许边缘设备在其各自的数据集内本地训练共享模型。

在前述部分中，提到了非独立同分布（Non-IID）数据的问题。然而，值得强调的是，FedAvg 算法本身并不具备有效解决由非独立同分布数据导致的模型分歧问题的能力，尤其是在采用复杂模型如神经网络的联邦学习情境中。当前，为了解决水平 FL 中的非独立同分布问题，研究学者们提出了一系列解决方案，这些方法主要包括基于数据、基于算法和基于系统的不同途径，具体细节如图 1 所示<sup>[4]</sup>。

### 2.1 基于数据的方法

一些研究专注于减轻非独立同分布对模型学习的影响，它们通过对数据进行调整或重新采样来实现这一目标。这些方法可能涵盖对数据的重加权、过采样或欠采样等策略，以使不同设备上的数据更加相似。这种调整的目的是降低数据分布的差异，从而有助于应对非独立同分布可能带来的学习分歧。

数据共享是在水平联邦学习中处理非独立同分布数据的一种直观而有效的方法<sup>[5]</sup>。该方法涉及在服务器上存储一个具有均匀分布的全局共享数据集  $G$ ，通过对  $G$  进行训练来预热全局模型。但它存在明显的缺点。首先，很难获得所谓均匀分布的全局数据集。其次，将部分全局数据下载到每个客户端进行模型训练违反了隐私保护学习的要求，这是联邦学习的基本动机。

数据增强最初是一种通过一些随机变换或知识传递来增加训练数据多样性的技术，它也可以用于缓解联邦学习中的本地数据不平衡问题。在联邦学习中，有三种主要的数据增强方法：基本方法、mixup 方法<sup>[6]</sup>和基于生成对抗网络 (GAN)<sup>[7]</sup> 的方法。

使用基本数据增强的基本思想在<sup>[8]</sup>中提出，其中每个客户端需要向服务器发送其标签分布信息，如每个类别的数据样本数量。然后，服务器可以计算每个数据类别的样本数及其均值，原始本地数据样本和增强数据均用于更新本地模型参数。mixup 方法是处理非独立同分布数据的另一种数据增强方

法。Shin 等人<sup>[9]</sup>首次使用该方法提出了 XorMixFL 框架。其核心思想是，每个客户端将其编码的种子样本（使用 XOR 运算符进行编码）上传到服务器进行解码，服务器上的基础数据样本以及解码后的样本可以构建一个新的平衡数据集。之后，在这个重构的数据上训练全局模型，并下载到每个客户端，直到训练收敛。Yoon 等人提出了一种均值增强方法<sup>[10]</sup>，通过与服务器交换批次本地数据的均值来降低本地数据不平衡的程度，最后将交换的均值数据组合并发送回每个客户端。

不同于前两种方法，联邦生成对抗网络（GAN）数据增强的目的是在非独立同分布数据存在的情况下训练一个良好的生成器。一般的方法是，每个客户端首先需要将其本地的种子数据样本发送到服务器，就像在数据共享策略中一样。然后，服务器可以基于这些种子样本训练 GAN 的生成器和判别器，而训练好的生成器将被发送到所有连接的客户端。

## 2.2 基于算法的方法

在联邦学习中，尽管目标是在不共享私有数据的情况下共同训练一个模型，但联邦学习的局部模型在性能上可能受到共享模型的影响。为了解决这些问题，最近个性化方法受到了广泛关注，个性化的目标是根据本地任务调整模型。一般来说，有几种主要类型的个性化方法，包括进行本地微调（通过正则化和插值或元学习进行个性化）、个性化层、多任务学习和知识蒸馏 [29]。

在进行微调的共同思想之一是基于元学习方法构建高质量的初始全局模型。代表性的方法之一是 Personalized FedAvg (Per-FedAvg)<sup>[11]</sup>。类似地，Jiang 等人将 Reptile 算法与 FedAvg 结合<sup>[12]</sup>，用于局部个性化，但是该方法的性能仅在 EMNIST-62 和 MNIST 数据集上进行了验证。Chen 等人提出了联邦元学习（FedMeta）框架<sup>[13]</sup>，其中元学习器在客户端之间共享，而不是使用全局模型。

个性化层方法允许每个客户端在神经网络模型中拥有个性化层，一种典型的范例称为 FedPer，其中基础层是神经网络的浅层，用于提取高层表示，而个性化层是用于分类的深层<sup>[14]</sup>。相比之下，Liang 等人提出了一个 LG-FEDAVG<sup>[15]</sup>，其中个性化层是神经网络的浅层，而与服务器共享的基础层是用于分类的深层。解决个性化问题的另一种方法是将其视为多任务学习问题。例如，MOCHA 是联邦多任务学习（FMTL）的代表性框架，首次考虑了 FL 的通信成本、stragglers 和容错问题<sup>[16]</sup>。Sattler 等人提出了一个非凸的 FMTL 框架，称为集群联邦学习（CFL），以对本地信息进行分组<sup>[17]</sup>。知识蒸馏也是个性化联邦学习的一种有前景的方法，在 FL 中，主要动机是将知识从服务器或其他客户端传递到某个客户端，以提高其在未知异构数据上的性能。

## 2.3 基于系统的方法

在联邦学习中，大多数方法假定整个系统只包含一个全局模型，这在异构数据环境中尤其难以学习所有客户端的信息。因此，提出了客户端聚类方法，通过将客户端分组到不同的簇中构建多中心框架。那些具有相似本地训练数据的客户端被分配到同一簇。这种方法有助于减轻不同训练数据之间的负面知识传递，提高了共享模型的性能。为了评估客户端之间的数据相似性，研究者们引入了两种主要的安全数据相似性评估方法。一种是通过比较不同簇模型的损失值来评估相似性，另一种是通过评估本地模型权重的相似性。这有助于在保持数据私密性的同时进行客户端聚类。这些系统级优化方法为解决联邦学习中的非独立同分布数据问题提供了实用的框架，以提高模型的性能和整体系统的鲁棒性。然而，这些方法在计算和通信资源方面可能需要额外的成本。

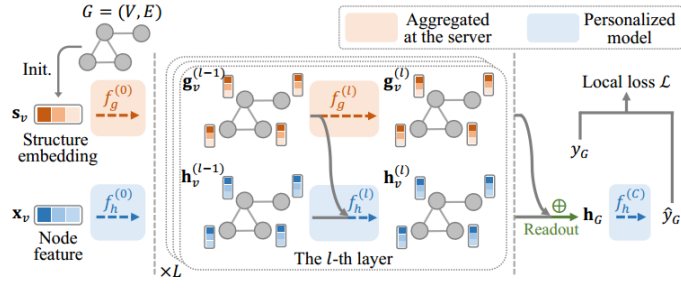


图 2: Feature-structure decoupled GNN

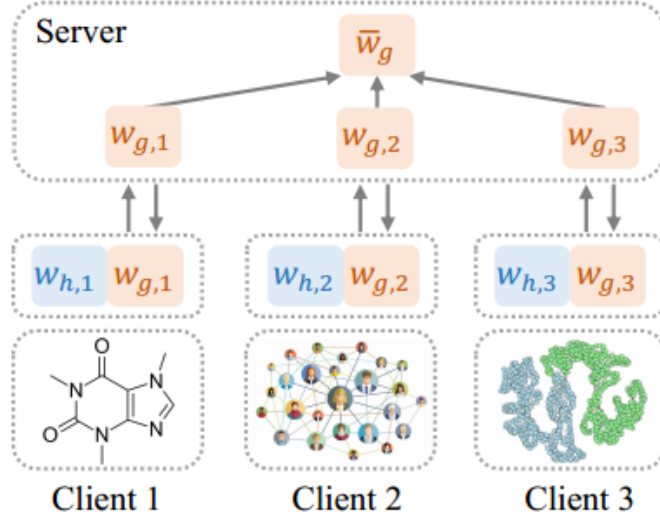


图 3: Model aggregation scheme

### 3 本文方法

#### 3.1 本文方法概述

本文方法 FedStar，这是一种用于联邦图学习（Federated Graph Learning, FGL）的框架，旨在克服在分布式环境中训练强大图神经网络（Graph Neural Networks, GNNs）模型时面临的挑战。FGL 允许客户端在不共享私有数据的情况下利用联邦学习的优势，分布式地训练 GNN 模型。

对于非独立同分布问题，这在真实世界的图数据中也是普遍存在的。观察真实图数据集，我们发现一些结构属性是多个领域共享的，受此启发，我们提出了 FedStar 框架，用于提取和共享不同图之间的通用底层结构信息。

为了明确提取结构信息而不是将其与节点特征一起编码，我们定义了结构嵌入并使用独立的结构编码器对其进行编码。然后，结构编码器在客户端之间共享，而基于特征的知识以个性化的方式进行学习，使得 FedStar 能够捕获更多基于结构的领域不变信息并避免特征不对齐的问题。本文中提出的 FedStar 框架的局部 GNN 架构概述如图 2 所示，在该架构中，蓝色框表示在本地训练并为每个客户个性化定制的模型，而橙色框表示在服务器上聚合的模型，其知识在客户端之间共享。图 3 部分展示了数据分布和模型聚合方案的示意图。这一方案有助于在联邦学习环境中有效地处理图数据，实现模型的分布式训练和知识共享。

#### 3.2 结构嵌入初始化

在传统的图神经网络（GNN）中，结构信息通常通过特征聚合的过程隐式地编码到节点表示中，同时包含了特征信息。然而，在非独立同分布的联邦图学习场景中，由于特征通常在不同领域之间是

异构的，很难将通用结构信息（例如节点度）统一编码到来自不同空间的基于特征的表示中。为了弥补这一差距，我们引入了一种新型的节点级信息载体，即结构嵌入，以显式地以向量形式表示通用结构知识。结构嵌入可以从图结构中初始化，并在消息聚合期间充当“特征”的角色。在这种情况下，结构信息是独立于特征信息学习的。

为了捕捉通用和全面的结构信息，在 FedStar 中，我们构建了结构嵌入，结合了本地和全局结构模式。具体而言，为了捕捉局部结构知识，我们引入了基于度的结构嵌入（DSE），如公式 1，它使用节点度的独热编码形式。对于图中的节点  $v$ ，其 DSE 表示为其中  $d_v$  是节点  $v$  的度， $I$  是单位函数， $k_1$  是 DSE 的维度。

$$\mathbf{s}_v^{\text{DSE}} = [\mathbb{I}(d_v = 1), \mathbb{I}(d_v = 2), \dots, \mathbb{I}(d_v \geq k_1)] \in \mathbb{R}^{k_1} \quad (1)$$

为了捕获全局结构知识，引入了基于随机游走的结构嵌入（RWSE），它是基于随机游走扩散过程计算的，具体为公式 2 所示。

$$\mathbf{s}_v^{\text{RWSE}} = [\mathbf{T}_{ii}, \mathbf{T}_{ii}^2, \dots, \mathbf{T}_{ii}^{k_2}] \in \mathbb{R}^{k_2} \quad (2)$$

其中， $T = AD^{-1}$  是由二进制邻接矩阵  $A$  和对角度数矩阵  $D$  计算得到的随机游走转移矩阵， $i$  是节点  $v$  的索引， $k_2$  是 RWSE 的维度，表示在扩散过程中涉及  $k_2$  跳内的邻居节点，并对结构表示  $s_{RWSE}^v$  有贡献。 $s_{RWSE}^v$  的第  $k$  个元素指的是节点  $v$  在  $k$  步随机游走中着陆到自身的概率。与专注于局部几何属性的 DSE 不同，RWSE 从全局角度描述节点的独特角色（例如，尾节点或中心节点）。此外，RWSE 能够整合领域不变的结构信息，例如在不同跳数的邻域分布。

最终，通过连接 DSE 和 RWSE，可以得到结构嵌入，如公式 3。

$$\mathbf{s}_v = \text{concat}[\mathbf{s}_v^{\text{DSE}}, \mathbf{s}_v^{\text{RWSE}}]. \quad (3)$$

### 3.3 特征-结构解耦的 GNN

在传统的联邦图学习（FGL）框架中，常常采用单通道图神经网络（GNNs）如 GraphSAGE 和 GIN，它们通过特征聚合的方式将结构信息隐式地编码到节点表示中。然而，在 FGL 中，尤其是在跨图任务中，客户端的本地数据集通常来自不同领域，导致不同特征分布。如果直接构建和共享基于特征的编码器，由于特征空间不一致，会影响个性化性能。为了解决这一问题，我们提出了一种特征-结构分离的 GNN。它使用两个并行通道分别学习属性和结构知识。在基于特征的通道中，特征编码器从原始节点特征中学习，并通过在每一层中聚合相邻属性和结构信息生成隐藏嵌入。同时，在基于结构的通道中，结构编码器在结构嵌入之上学习，并在整个图上传播结构信息。所提出的 GNN 的概述如图 2 所示。

该 GNN 模型由三个主要部分组成：(i) 具有可学习参数的线性层，负责初始输入的计算；(ii) 多层的特征-结构分离 GNN 层，其中特征编码器和结构编码器分别学习节点特征和结构信息；(iii) 分类器，用于图分类任务。通过堆叠这些层，GNN 能够学习节点级别的特征和结构嵌入，最终生成图级别的嵌入。在图级别嵌入生成后，采用交叉熵损失对本地模型进行优化。每个客户端具有一组可学习的参数，包括特征编码器、结构编码器和分类器的参数。这种结构使得 GNN 能够在非独立同分布的图数据上学习通用的特征和结构信息，为联邦学习任务提供了强大的表示学习能力。

### 3.4 结构知识共享

FedStar 通过结构嵌入和结构编码器捕获的通用结构信息，促进了在具有不同领域图数据的客户端之间共享学到的结构知识。训练范式涉及到每个客户端拥有来自不同领域的图数据，每个客户端都采用相同的模型架构。每个客户端的本地模型被明确分解为两个子模型：特征编码器（ $w_{h,m}$ ）和结构编码器（ $w_{g,m}$ ）。关键创新点在于在联邦学习（FL）框架中共享结构编码器参数（ $w_{g,m}$ ），同时允许特征编码器在本地进行训练。

训练过程遵循 FedAvg 类似的迭代过程。客户端传输其结构编码器参数到服务器，在服务器上通过基于每个客户端本地数据集中图数量的加权平均计算全局结构编码器（ $w_g$ ）。然后，服务器将  $w_g$  发送回客户端，客户端使用  $w_g$  更新其本地结构编码器，并开始下一轮的本地训练。这种结构知识共享机制使得客户端能够建立一个通用的结构编码器，强调了在没有特征信息的情况下捕获域不变模式。

通过对结构基础编码器的迭代训练和聚合，FedStar 在来自不同领域的非独立同分布图上泛化了结构知识。全局共享的结构知识增强了各个客户端的特定学习任务。在每一层将基于结构的嵌入与基于特征的嵌入相连接，确保了全局共享的结构知识引导了特征学习过程，提供了额外的结构感知信息。总体而言，FedStar 的结构知识共享方案使得联邦图学习框架能够发现共同的结构知识，并提升了特定领域特征学习的表征能力。

## 4 复现细节

### 4.1 与已有开源代码对比

代码基本源于作者改论文源码，解决部分 bug 跑通代码，并做了部分改动。

---

**Procedure 1** FedStar (Federated Graph Learning via Structural Knowledge Sharing)

---

**Server input:** Initial structure GNN encoder  $\bar{w}_g$ ;

**Client  $m$ 's input:** Initial feature GNN encoder  $w_{h,m}$ , local labeled graph dataset  $D_m$ ;

**Server executes:**

- 1: Communicate  $\bar{w}_g$  to all clients  $m \in [1, M]$ ;
  - 2: **for** each round  $T = 1, 2, \dots$  **do**
  - 3:     **for** each client  $m$  in parallel **do**
  - 4:          $w_{g,m} \leftarrow \text{LocalUpdate}(m, \bar{w}_g)$ ;
  - 5:     **end for**
  - 6:     Update structure encoder by  $\bar{w}_g = \sum_{m=1}^M \frac{|D_m|}{N} w_{g,m}$ ;
  - 7: **end for**
  - 8: **function** LocalUpdate( $m, \bar{w}_g$ )
  - 9:     Initialize  $w_{g,m} \leftarrow \bar{w}_g$ ;
  - 10:    **for** each local epoch **do**
  - 11:       Update local model by  $w_{h,m}^*, w_{g,m}^* = \arg \min_{w_{h,m}, w_{g,m}} L_m(w_m, D_m)$ ;
  - 12:    **end for**
  - 13:    **return**  $w_{g,m}^*$ ;
  - 14: **end function**
- 

### 4.2 实验环境搭建

numpy

pandas

sklearn

dtaidistance



torch==1.11.0  
torchvision==0.12.0  
torchaudio==0.11.0  
torch-scatter==2.0.9  
torch-sparse==0.6.13  
torch-geometric==2.

### 4.3 创新点

将 FedStar 联邦学习框架中引入 FedPer 的联邦机制，实现更加个性化、灵活和高效的模型训练和更新。在训练模型时，将参与服务器端的本地网络模型分为基本层和个性化层，所有的客户设备共享基本层，共享相同的权重，这些权重来自参数服务器。

## 5 实验结果分析

### 5.1 数据集

| domains             | datasets    | Graphs | Classes |
|---------------------|-------------|--------|---------|
| SM(Small Molecules) | MUTAG       | 188    | 2       |
|                     | BZR         | 405    | 2       |
|                     | COX2        | 467    | 2       |
|                     | DHFR        | 756    | 2       |
|                     | PTC-MR      | 344    | 2       |
|                     | AIDS        | 2000   | 2       |
|                     | NCI1        | 4110   | 2       |
| BIO(Bioinformatics) | ENZYMES     | 600    | 6       |
|                     | DD          | 1178   | 2       |
|                     | PROTEINS    | 1113   | 2       |
| SN(Social Networks) | COLLAB      | 5000   | 3       |
|                     | IMDB-BINARY | 1000   | 2       |
|                     | IMDB-MULTI  | 1500   | 3       |
| CV(Computer Vision) | Letter-low  | 2250   | 15      |
|                     | Letter-high | 2250   | 15      |
|                     | Letter-med  | 2250   | 15      |

表 1: datasets

本文使用了 16 个公共图分类数据集，如表 1 所示，涵盖了四个不同领域的的数据，分别是小分子（MUTAG、BZR、COX2、DHFR、PTC MR、AIDS、NCI1）、生物信息学（ENZYMES、DD、PROTEINS）、社交网络（COLLAB、IMDB-BINARY、IMDB-MULTI）以及计算机视觉（Letter-low、Letter-high、Letter-med）。同时为了模拟联邦图学习中的数据异质性，创建了四个非独立同分布（Non-IID）的设置，具体如下：CHEM 基于七个小分子数据集的跨数据集设置，基于来自两个或三个域的数据集的跨域设置 BIO-CHEM，BIO-CHEM-SN，BIO-SN-CV。这样的设置旨在模拟在联邦图学习中可能出现的数据异质性。

### 5.2 基线方法

将 FedStar 与六个基线进行比较，包括：

Local，简单直观，无需通信，客户端可在本地独立训练模型。



FedAvg<sup>[3]</sup>, 标准 FL 算法, 广泛应用, 但对异质性数据和不平衡分布处理有限。

FedProx<sup>[18]</sup>, 专注处理 FL 异质性问题, 通过添加正则项促使客户端模型更一致, 算法相对复杂。

FedPer<sup>[14]</sup>, 针对 FL 异质性问题, 引入个性化因子以调整客户端贡献, 致力于更好平衡模型性能。

FedSage<sup>[19]</sup>, 利用图神经网络, 处理复杂关系和异质性数据, 但受制于图结构表示。

GCFL<sup>[20]</sup>, 利用图卷积网络等技术, 适用于复杂数据关系, 可能对计算资源要求较高。

### 5.3 实验结果及分析

表 2: 实验结果

| Setting ( domains) | SM           |             | BIO-SM       |             | BIO-SM-SN    |             | BIO-SN-CV    |             |
|--------------------|--------------|-------------|--------------|-------------|--------------|-------------|--------------|-------------|
| Accuracy           | avg.         | avg.gain    | avg.         | avg.gain    | avg.         | avg.gain    | avg.         | avg.gain    |
| Local              | 75.38        | -           | 71.09        | -           | 69.37        | -           | 66.91        | -           |
| FedAvg             | 75.26        | -0.13       | 70.65        | -0.44       | 68.92        | -0.45       | 64.86        | -2.05       |
| FedProx            | 75.30        | -0.08       | 70.75        | -0.34       | 69.21        | -0.16       | 65.18        | -1.72       |
| FedPer             | 77.09        | 1.70        | 71.97        | 0.88        | 69.37        | -0.01       | 62.23        | -4.67       |
| FedSage            | 75.90        | 0.51        | 70.34        | -0.74       | 69.55        | 0.18        | 67.95        | 1.04        |
| GCFL               | 76.49        | 1.11        | 71.60        | 0.51        | 70.65        | 1.28        | 66.31        | -0.60       |
| FedStar            | 79.79        | 4.41        | 74.54        | 3.46        | 72.16        | 2.78        | 69.49        | 2.58        |
| <b>FedStar(me)</b> | <b>78.81</b> | <b>3.34</b> | <b>74.27</b> | <b>3.18</b> | <b>71.79</b> | <b>2.42</b> | <b>67.59</b> | <b>0.68</b> |

实验结果如表 2 所示, 显示了该方法模型在各个数据集上的出色表现。尤其值得注意的是, 在实验结果中, 跨数据集但不跨领域的小分子数据设置中取得的结果精度最高, 这强有力地证明了在这种非独立同分布条件下, 该方法相较于跨领域的数据集, 能够实现更为卓越的训练效果。

为了深入分析不同数据集训练结果精度不同的原因, 我们进行了进一步的数据集分析。从数据集的图数量、节点属性贡献以及平均节点和边数三个角度入手, 我们详细研究了 16 个数据集的训练情况。具体而言, 我们发现数据集 AIDS 在测试效果方面表现最佳, 达到了 99.60% 的准确度。进一步观察该数据集的信息, 我们发现它包含大量的图, 且平均节点数和边数既不过少也不过多。此外, 该数据集提供了节点的属性贡献, 从而能够获得更好的训练效果。相反, 考虑另一个数据集 PTC\_MR, 虽然同样为 2 分类问题, 但该数据集只包含三百多个图, 且缺乏节点属性贡献。因此, 最终的训练效果仅能达到 50.00% 左右。

总结表格中相同数据集设置下, 与原论文的联邦图分类实验结果以及我个人复现的成果相比较的平均增益。结果表明, FedStarz 在性能上整体优于其他基线方法, 尽管复现结果相较原论文略微下降。这或许是由于本地训练受限所致。考虑到这一点, 若能进一步增加训练轮次和参数调整, 并将创新点融入其中, 有望提高最终的训练效果。

## 6 总结与展望

在复现 FedStar 论文的过程中, 首次尝试了对联邦学习中的图分类问题进行全面复现。FedStar 提出了一种创新性的联邦学习方法, 通过结构知识共享解决了非独立同分布问题。该方法基于结构嵌入和特征-结构解耦的图神经网络 (GNN), 明确地表示并充分捕获了数据中的结构知识, 而不受基于特征的信息的干扰。这一策略使得来自不同领域的客户端能够在全局范围内学习到与领域无关的结构知识, 通过这种方式, 我们有效地区分了图的结构特征, 使得模型更加专注于学习和理解数据之间的内在关系。

在大量实验中, FedStar 在公共数据集上展现了出色的有效性。然而, 复现过程中也揭示了一些

挑战和不足之处。尽管本次复现取得了一定的成功，但仍然存在对于一些细节和创新点理解不够深刻的问题。在未来的工作中，计划探索对与 FedPer 联邦学习机制的融合或采用其它先进的图神经网络结构，如 GraphSAGE、GAT 等。通过将我们的结构知识共享框架与 FedPer 的个性化学习策略相结合，期望能够更好地适应每个客户端的特定数据分布，进一步提高在非独立同分布情境下的性能表现。

同时，本人认识到复现任务中的原创性工作存在不足，尚未涉及独立实现代码和缺少创新性想法。为了提升个人能力和深化理解，将在学术研究和编程实践中加强学习锻炼，争取早日取得实质性的研究成果。这将包括更深入地理解 FedStar 论文中的方法，探索改进和创新的机会，以及更自主地开展代码实现。

## 参考文献

- [1] TAN Y, LIU Y, LONG G, et al. Federated learning on non-iid graphs via structural knowledge sharing [C]//Proceedings of the AAAI conference on artificial intelligence: vol. 37: 8. 2023: 9953-9961.
- [2] ZHANG C, XIE Y, BAI H, et al. A survey on federated learning[J]. Knowledge-Based Systems, 2021, 216: 106775.
- [3] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. 2017: 1273-1282.
- [4] ZHU H, XU J, LIU S, et al. Federated learning on non-IID data: A survey[J]. Neurocomputing, 2021, 465: 371-390.
- [5] ZHAO Y, LI M, LAI L, et al. Federated learning with non-iid data[J]. arXiv preprint arXiv:1806.00582, 2018.
- [6] ZHANG H, Cissé M, DAUPHIN Y, et al. Mixup: Beyond Empirical Risk Minimization. BT-6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30-May 3, 2018, Conference Track Proceedings[J]., 2018.
- [7] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial nets[J]. Advances in neural information processing systems, 2014, 27.
- [8] DUAN M, LIU D, CHEN X, et al. Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications[C]//2019 IEEE 37th international conference on computer design (ICCD). 2019: 246-254.
- [9] SHIN M, HWANG C, KIM J, et al. Xor mixup: Privacy-preserving data augmentation for one-shot federated learning[J]. arXiv preprint arXiv:2006.05148, 2020.
- [10] YOON T, SHIN S, HWANG S J, et al. Fedmix: Approximation of mixup under mean augmented federated learning[J]. arXiv preprint arXiv:2107.00233, 2021.
- [11] FALLAH A, MOKHTARI A, OZDAGLAR A. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach[J]. Advances in Neural Information Processing Systems, 2020, 33: 3557-3568.

- [12] JIANG Y, KONEČNÝ J, RUSH K, et al. Improving federated learning personalization via model agnostic meta learning[J]. arXiv preprint arXiv:1909.12488, 2019.
- [13] CHEN F, LUO M, DONG Z, et al. Federated meta-learning with fast convergence and efficient communication[J]. arXiv preprint arXiv:1802.07876, 2018.
- [14] ARIVAZHAGAN M G, AGGARWAL V, SINGH A K, et al. Federated learning with personalization layers[J]. arXiv preprint arXiv:1912.00818, 2019.
- [15] LIANG P P, LIU T, ZIYIN L, et al. Think locally, act globally: Federated learning with local and global representations[J]. arXiv preprint arXiv:2001.01523, 2020.
- [16] SMITH V, CHIANG C K, SANJABI M, et al. Federated multi-task learning[J]. Advances in neural information processing systems, 2017, 30.
- [17] SATTLER F, MÜLLER K R, SAMEK W. Clustered federated learning: Model-agnostic distributed multitask optimization under privacy constraints[J]. IEEE transactions on neural networks and learning systems, 2020, 32(8): 3710-3722.
- [18] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine learning and systems, 2020, 2: 429-450.
- [19] ZHANG K, YANG C, LI X, et al. Subgraph federated learning with missing neighbor generation[J]. Advances in Neural Information Processing Systems, 2021, 34: 6671-6682.
- [20] XIE H, MA J, XIONG L, et al. Federated graph classification over non-iid graphs[J]. Advances in Neural Information Processing Systems, 2021, 34: 18839-18852.