FEDBABU: TOWARD ENHANCED REPRESENTATION FOR FEDERATED IMAGE CLASSIFICATION

摘要

联邦学习已经发展到在数据异构下改进单个全局模型(把数据异构作为一种诅咒)，或者使用数据异构开发多个个性化模型(把数据异构作为一种祝福)。然而，目前很少有研究同时考虑这两个方向。在本文中，我们首先通过在客户端层面分析联邦平均来研究它们之间的关系，并确定更好的联邦全局模型性能并不能不断提高个性化。为了阐明这种个性化性能下降问题的原因，我们将整个网络分解为与通用性相关的主体(提取器)和与个性化相关的头部(分类器)。我们指出，这个问题源于对头部的训练。基于这一观察，我们提出了一种新的联邦学习算法，称为FedBABU，它在联邦训练期间只更新模型的主体(即头部随机初始化且从不更新)，并且在评估过程中对头部进行微调以实现个性化。大量的实验表明，FedBABU具有一致的性能改进和高效的个性化。

关键词：个性化联邦学习；动态正则化

1 引言

随着移动设备的普及和互联网的快速发展，人们在不同设备上产生的数据日益庞大且异构。在这种情况下，传统的集中式机器学习方法可能面临数据难以集中存储和隐私问题。因此，联邦学习作为一种分布式学习框架应运而生。联邦学习允许在设备上进行本地训练，而不必将原始数据传输到中央服务器。然而，在提高全局模型性能和实现个性化之间存在一个平衡问题，特别是在数据异构性方面。选题依据：过去的研究主要集中在改进单一全局模型或者在设备之间利用数据异构性开发多个个性化模型。然而，很少有研究同时考虑这两个方向。本选题基于对联邦平均算法的分析，发现提高全局模型性能并不能始终改善个性化，进一步探讨了这一现象的原因。研究者意识到这一问题源于对模型的头部进行训练，而联邦学习中对头部的训练可能会影响个性化的效果。因此，提出了一种新颖的算法FedBABU，通过在联邦训练期间仅更新模型的主体，实现更好的全局模型性能和更有效的个性化。

2 相关工作

2.1 单一全局模型的联邦学习

由McMahan等人（2017年） [1]提出的FedAvg，旨在学习一个单一全局模型，以在不将客户原始数据存储在中央服务器的情况下获得丰富数据的优势，从而通过本地更新降低通信成本。然而，对于来自各个客户端的非独立同分布（non-IID）的数据，开发出全局最优模型变得困难。为了解决这个问题，研究已经进行，使客户端的数据分布类似于IID，或者在本地更新过程中添加正则化以减小与全局模型的距离。

Zhao等人（2018年） [2]建议所有客户端共享一部分公共数据，而Duan等人（2019年） [3]则通过增加数据来平衡客户端的标签分布。最近有两项研究（Li等人，2018年 [4]；Acar等人，2021年 [5]）对具有与全局模型差异较大的本地模型进行惩罚，通过在本地优化过程中添加正则化项，使全局模型能够更可靠地收敛。然而，需要注意的是，使用以上方法训练的单一全局模型并不针对每个客户端进行优化。

2.2 个性化联邦学习

将主体和头部解耦以实现对每个客户端的个性化风格化。尽管可以在没有联邦的情况下开发本地模型，但这种方法受到数据限制的困扰。因此，为了保持联邦和个性化模型的好处，已经应用了许多其他方法于联邦学习中：聚类、多任务学习、迁移学习、正则化损失函数和元学习。两项研究（Briggs等人，2020年 [6]；Mansour等人，2020年 [7]）将相似的客户端聚类在一起，以匹配集群内的数据分布，并为每个集群学习单独的模型，而无需进行集群间的联邦。

2.3 将主体和头部解耦以实现个性化的联邦学习

将主体和头部解耦以实现个性化联邦学习的训练方案已在各个领域中得到应用，包括长尾识别、噪声标签学习以及元学习。在个性化联邦学习中，已经有尝试使用这种解耦方法的努力。为了保持一致的解释，我们从本地更新和聚合部分的角度描述每个算法。FedPer（Arivazhagan等人，2019年） [8]，类似于FedPav（Zhuang等人，2020年） [9]，在本地更新期间联合学习整个网络，只聚合底层。当底层与主体匹配时，主体在所有客户端共享，而头部则个性化到每个客户端。

3 本文方法

3.1 联邦学习训练过程

此部分对本文将要复现的工作进行概述，图的插入如图 **??**所示：定义四个阶段的联邦学习训练过程，包括客户端选择、广播初始化、本地更新和全局聚合。使用形式化符号表示各个阶段的操作，明确了参与通信轮次的客户端集合、参数初始化和本地模型更新的步骤。

3.2 参数解耦

将模型参数分解为主体（提取器）参数和头部（分类器）参数。这种参数解耦是本文算法的关键特征。

3.3 实验设置

主要使用MobileNet在CIFAR100数据集上进行实验。设置了100个客户端，每个客户端有500个训练数据和100个测试数据。客户端数据集的异构分布参考了McMahan等人（2017）的实验设置。控制了三个超参数：客户端比例f、本地轮次 τ 和每用户分片数s。

3.4 评估

计算了FedAvg和FedBABU的初始准确性和个性化准确性。遵循Wang等人（2019）提出的联邦个性化评估流程，包括将全局模型广播给所有客户端并在每个客户端的测试数据集上评估的初始准确性，以及使用每个客户端的训练数据集进行微调并在测试数据集上评估的个性化准确性。对其他个性化联邦学习算法（如FedPer、LG-FedAvg和FedRep）也进行了个性化准确性的计算。

3.5 环境控制

控制了FL环境的三个超参数，即客户端比例f、本地轮次 τ 和每用户分片数s。对学习率进行了控制，开始为0.1，并在总更新的一半和三分之三处按0.1的因子衰减。通过固定通信轮次和本地轮次的乘积为320，确保了所有实验的一致性。这个概括涵盖了您的研究方法，包括实验设置、训练过程和评估策略。在写论文时，您可以在每个部分详细说明方法的具体步骤、参数选择和实验设计。

4 复现细节

4.1 与已有开源代码对比

此次复现的论文作者提供了代码，但是原有代码略显复杂，我把代码按照自己的逻辑梳理，用自己的框架重写了一遍。并加了自己的改进，在原有的方法上，我使用了动态正则化的方式，提高准确率。即在有全局模型向量的情况下，计算了模型参数向量与全局模型向量之间的差异，并将这一差异添加到损失中。然后，减去了模型参数向量与旧梯度向量的点积，最终通过梯度下降方法来更新模型参数。这种方法的目的是通过正则化来影响模型训练，以适应全局模型。

5 实验结果分析

5.1 实验1

首先使用FedAvg算法和MobileNet架构对CIFAR100数据集进行实验，通过设置不同数据分布的异质性评估了模型在没有进行微调的情况和进行了五次微调周期后的初始准确度和个

性化准确度。

S=100		S=50		S=10	
Initial	Personalized	Initial	Personalized	Initial	Personalized
37.35	42.87	36.14	46.97	24.05	70.31

表 1. 不同异构程度数据下微调与未微调的准确度

5.2 实验2

在上个实验的基础上，通过引入参数p（服务器拥有的所有客户端数据的一小部分比例）在服务器上进行微调。实验的结果：提高了全局模型的初始准确性，但在数据异构性显著的情况下，个性化模型的准确度下降。

p	S=100		S=50		S=10	
	Initial	Personalized	Initial	Personalized	Initial	Personalized
0.05	29.14	32.46	27.31	34.43	18.24	54.55
0.10	30.62	33.43	29.52	35.52	19.25	49.48

表 2. 引入参数P后的准确度

5.3 实验3

可以看出，在几种异构数据下，FedBABU的准确率都是较好的

S	f	FedBABU	FedAvg	FedPer	LG-FedAvg	FedRep	Per-FedAvg	Ditto
100	0.1	48.22	40.52	43.85	38.69	19.91	45.95	43.16
50	0.1	57.02	48.77	51.37	41.44	29.77	41.63	41.07
10	0.1	73.77	67.15	68.42	53.40	59.31	30.58	32.12

表 3. 不同异构程度数据下不同方法的准确度对比

6 总结与展望

本研究展示了联邦学习在处理个性化图像分类任务中的有效性和优势。我们的实验结果表明，通过将网络模型解耦为主体和头部，并在本地客户端上进行有效的模型训练，可以在节约时间和计算资源的同时，获得与全参数训练相近的准确率。同时我引入了客户端控制参数，减少了客户端的漂移程度，使其朝着全局模型的方向前进。此外，我们的研究还揭示了ResNet在处理复杂图像分类任务时，相比于MobileNet，能够提供更高的识别准确率。这一发现对于未来在移动和边缘设备上部署高效且准确的联邦学习模型具有重要意义。然而，本研究也表明，即使在联邦学习环境中，模型选择和优化仍然是实现高效图像分类的关键因

素。未来的工作可以进一步探索不同类型的网络架构，以及它们在联邦学习环境下的性能表现，以期提高模型的准确性和适应性。

参考文献

[1] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, et al. Communication-efficient learning of deep networks from decentralized data. In *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, pages 1273–1282, 2017.

[2] Yue Zhao, Meng Li, Liangzhen Lai, Naveen Suda, Damon Civin, and Vikas Chandra. Federated learning with non-iid data. *arXiv preprint arXiv:1806.00582*, 2018.

[3] Moming Duan, Duo Liu, Xianzhang Chen, Yujuan Tan, Jinting Ren, Lei Qiao, and Liang Liang. Astraea: Self-balancing federated learning for improving classification accuracy of mobile deep learning applications. In *2019 IEEE 37th International Conference on Computer Design (ICCD)*, pages 246–254. IEEE, 2019.

[4] Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *arXiv preprint arXiv:1812.06127*, 2018.

[5] Durmus Alp Emre Acar, Yue Zhao, Ramon Matas Navarro, Matthew Mattina, Paul N. Whatmough, and Venkatesh Saligrama. Federated learning based on dynamic regularization. In *International Conference on Learning Representations*, 2021.

[6] Christopher Briggs, Zhong Fan, and Peter Andras. Federated learning with hierarchical clustering of local updates to improve training on non-iid data. In *2020 International Joint Conference on Neural Networks (IJCNN)*, pages 1–9. IEEE, 2020.

[7] Yishay Mansour, Mehryar Mohri, Jae Ro, and Ananda Theertha Suresh. Three approaches for personalization with applications to federated learning. *arXiv preprint arXiv:2002.10619*, 2020.

[8] Manoj Ghuhan Arivazhagan, Vinay Aggarwal, Aaditya Kumar Singh, and Sunav Choudhary. Federated learning with personalization layers. *arXiv preprint arXiv:1912.00818*, 2019.

[9] Weiming Zhuang, Yonggang Wen, Xuesen Zhang, Xin Gan, Daiying Yin, Dongzhan Zhou, Shuai Zhang, and Shuai Yi. Performance optimization of federated person re-identification via benchmark analysis. In *Proceedings of the 28th ACM International Conference on Multimedia*, pages 955–963, 2020.