联邦相互学习：一种针对异构数据、模型和目标的协同机器学习方法

沈弢[1]，张杰[2]，贾鑫康[2]，张凤达[1]，吕喆奇[1]，况琨[1]，吴超[3]，吴飞[1]
[1]浙江大学计算机科学与技术学院，中国杭州市，310027
[2]浙江大学软件学院，中国杭州市，310027
[3]浙江大学公共管理学院，中国杭州市，310027

摘要：联邦学习（FL）是深度学习中的一种新技术，可以让客户端在保留各自隐私数据的情况下协同训练模型。然而，由于每个客户端的数据分布、算力和场景都不同，联邦学习面临客户端异构环境的挑战。现有方法（如FedAvg）无法有效满足每个客户的定制化需求。为解决联邦学习中的异构挑战，本文首先详述了数据、模型和目标（DMO）这3个主要异构来源，然后提出一种新的联邦相互学习（FML）框架。该框架使得每个客户端都能训练一个考虑到数据异构（DH）的个性化模型。在模型异构（MH）问题上，引入一种“模因模型”作为个性化模型与全局模型之间的中介，并且采用深度相互学习（DML）的知识蒸馏技术在两个异构模型之间传递知识。针对目标异构（OH）问题，通过共享部分模型参数，设计针对特定任务的个性化模型，同时，利用模因模型进行相互学习。本研究通过实验评估了FML在应对DMO异构性方面的表现，并与其他常见FL方法在相似场景下进行对比。实验结果表明，FML在处理FL环境中的DMO问题的表现卓越，优于其他方法。

关键词：联邦学习；知识蒸馏；隐私保护；异构环境
https://doi.org/10.1631/FITEE.2300098