去中心化联邦学习保护区模型和数据隐私

本文提出了一种完全分散的方法，它允许在训练有素的模型之间共享知识。这依赖于分配给模型的教师和学生角色，通过综合生成的输入数据，学生可以根据教师的输出进行训练。

迁移学习 + 联邦学习

迁移学习：把已训练好的模型（预训练模型）参数迁移到新的模型来帮助新模型训练。

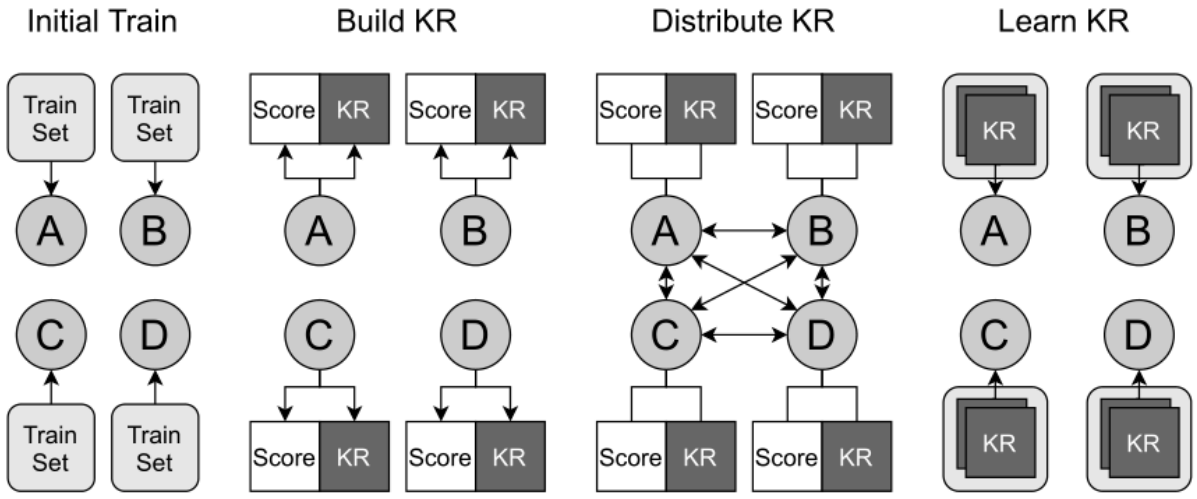
培训过程：

每个模型都可以扮演学生或老师的角色。教师模型通过提供知识表示来训练学生模型。
首先，我们假设有一组模型，每个模型在它们自己的本地环境中执行相同的任务。这些模型基于相同的目标进行训练，但只使用本地可用的训练数据。
为了防止培训数据或模型参数在不同环境之间的共享，模型调整教师的角色，以在其他环境中训练学生模型。

训练步骤:

(1)初始训练;
(2)教师角色调整与知识表示构建;
(3)知识表示分配;
(4)适应学生角色，培训教师知识表达能力;

最初，所有模型都是在本地可用的训练数据上训练的。然后，模型对教师角色进行调整，分别生成知识表示。
从而，从本地可用的训练数据的取值范围生成辅助输入数据。这个范围必须在所有环境中同步。否则，没有与原始的本地训练数据的连接，这些数据用于在他们的环境中训练模型。
此外，还会计算出反映模型在任务上执行情况的分数。接下来，分布知识表示。在接收到知识表示之后，模型会检查附加的分数，并将其与本地分数进行比较。分数较低的代表将被删除。当得到更高或相同的分数时，模型会调整学生的角色，并根据所接收到的知识表示进行训练。通过这个过程，每个模型将被重新训练和更新。



结论：

实验表明，该算法能够在分布式系统中训练具有相同配置的不同模型。该方法通过使用辅助样本在模型之间传递知识来保护数据隐私。不需要训练过程同步的中心实例。模型参数和梯度都不需要转移。