

FEDERATED TRAINING METHOD AND APPARATUS, AND COMPUTER SYSTEM

联邦训练的方法、装置及计算机系统

说明书

5

技术领域

本说明书一个或多个实施例涉及计算机技术领域，尤其涉及一种联邦训练的方法、装置及计算机系统。

10

背景技术

随着人工智能和大数据时代的到来，机器学习（Machine Learning）技术各个领域得到了广泛的应用。然而，由于数据的安全性和隐私保护等问题，传统的集中式机器学习方法面临着诸多限制。于是，联邦学习（Federated Learning）应运而生。

15

联邦学习（或称联邦训练）是一种分布式机器学习技术，它允许多个参与方在保护数据隐私的前提下进行模型训练。每个参与方只在本地维护自己的数据集，并通过联邦学习算法交换部分的模型更新参数，从而实现模型的联合训练。联邦学习因其保护数据隐私和保密性的特性，被广泛应用于医疗、金融、物联网等领域。

20

由此，本说明书实施例披露一种联邦训练方案，可以更好地满足实际应用中的需求，例如，在保护数据隐私的前提下，提高模型的泛化性能和可用性。

发明内容

本说明书一个或多个实施例描述了联邦训练方法和对应装置，以满足实际应用中对联邦学习性能和效果的更高要求。

25

根据第一方面，提供了一种联邦训练方法，涉及中间方和 n 个参与方，所述方法应用于所述中间方，所述方法涉及的任一轮迭代训练包括：从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

根据第二方面，提供了一种联邦训练装置，涉及中间方和 n 个参与方，所述装置集成于所述中间方，所述装置通过以下模块执行任一轮迭代训练：嵌入表征接收单元，配置为从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；权重预测单元，配置为针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；结果预测单元，配置为利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

根据第三方面，提供了一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器集成于中间方，所述中间方和多个参与方协同进行联邦训练；所述处理器执行所述程序时实现任一轮迭代训练中的如下步骤：从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

根据第四方面，提供了一种计算设备，包括存储器和处理器，其中所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面提供的方法。

采用本说明书实施例提供的方法和装置，通过共享底层网络结构，以及为不同任务设置用于聚合中间结果的不同门控网络，实现了不同任务的数据特征的联合学习和模型参数共享，从而有效提升了模型的泛化能力。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述中所需使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

图 1 为本说明书实施例披露的联邦训练方案的实施架构示意图；

图 2 为本说明书实施例披露的联邦训练方法涉及的中间方和 n 个参与方之间的通信交互示意图；

图 3 为本说明书实施例披露的联邦训练装置集成于中间方时的功能结构示意图；

图 4 为本说明书实施例提供的计算机系统的结构示意图。

具体实施方式

下面结合附图，对本说明书提供的方案进行描述。

承前所述，联邦学习因其保护数据隐私和保密性的特性，被广泛应用于医疗、金融、物联网等领域。然而在许多应用领域，联邦学习的各参与方关注不同的模型任务（或称预测任务）。比如说，在电子支付领域，假设联邦学习的参与方是两个电子钱包，其中钱包 A 的业务主要是为商户提供收款和支付服务，因此，其关注的模型任务是对非法资金转移等欺诈手段的检测，钱包 B 的业务主要是提供个人间的转账和支付服务，因此，其关注的模型任务是对用户的信用评估。

由此提出，在联邦学习框架下实现多个相关任务的预测。具体，本说明书实施例关注的是纵向联邦学习框架下的多任务学习。可以理解，在纵向联邦学习框架下，不同参与方拥有各自的数据集，这些数据集在样本维度上存在重叠，但在特征维度上相互独立，也即，不同参与方拥有相同的样本空间和不同的特征空间，换言之，多个参与方持有相同样本的不同特征部分。

在传统的纵向联邦学习中，多个参与方（或称多个数据方）各自利用本地模型（bottom model）处理相同样本的不同特征部分，得到对应的中间结果，并传递给中间方，中间方在对中间结果进行聚合后，利用其部署的顶部模型（top model）继续进行前馈处理，得到针对全局任务的预测结果，从而利用预测结果和对应的样本标签计算训练损失，通过反向传播，使得中间方和多个参与方能够各自更新本方部署的模型。

为了实现纵向联邦学习框架下的多任务学习，考虑针对各个模型任务分别建立联邦学习流程，从而得到针对多个预测任务的多个全局模型。比如说，假定有 2 个参与方和 3 个预测任务，此时，2 个参与方各自针对 3 个预测任务部署 3 个本地模型，中间方针对 3 个预测任务部署 3 个顶部模型。然而，此种方式在每个任务的标注数据较少时，对于每个任务训练的全局模型的泛化能力较弱，而且，整体产生的通信量较大。

基于以上观察和分析，申请人提出一种联邦训练方案。在此方案中，多个（记作 n 个）参与方各自只需在本地部署一个本地模型，中间方针对多个（记作 m 个）预测任务配置 m 套门控网络-预测网络，其中任意的第 j 个门控网络用于确定 n 个参与方针对某个样本上传的 n 个中间结果（或称样本表征）的权重，此权重用于对 n 个中间结果进行聚合；第 j 个预测网络用于对聚合结果进行处理，得到第 j 个任务下的预测结果，从而基于该预测结果和对应的样本标签实现对方模型的更新。图 1 中以 $n=2$ ， $m=2$ 为例，示意方案架构。

如此，可以实现在保护隐私的前提下同时处理不同相关任务的数据，并通过共享底层

网络结构，实现了不同任务数据特征的联合学习和模型参数共享，可以有效提升模型的泛化能力，并减少训练产生的通信量。

需说明，上述联邦训练方案具有广阔的应用场景，可以广泛应用于需要处理多个相关任务且涉及数据隐私保护的场景。为帮助理解，下面先结合具体的应用场景，介绍多个参与方中训练数据的分布，再介绍上述联邦训练方案的具体实施步骤。

5 与方中训练数据的分布，再介绍上述联邦训练方案的具体实施步骤。

场景 1：在智能交通领域，多个参与方共同学习多个城市的交通数据，执行针对交通流量的预测任务和针对交通事故的预测任务。

具体地，任一训练样本对应一个特定的时间点或时间段，多个参与方各自持有的样本特征部分是该时间点或时间段下的交通数据记录。示例性的，各个参与方可以实例化为存储有对应城市交通数据的服务器集群，交通数据记录可以通过交通摄像头、传感器、GPS 设备等采集而得到。

场景 2：在电子商务领域，多个电商平台共同学习各平台的用户数据，从而提高更准确的个性化商品推荐和广告推送服务。

具体地，任一训练样本对应一个用户，多个电商平台各自持有该用户在对平台中的历史交易数据等。需说明，文中提及的与用户相关的数据，均是在用户确认授权后进行采集和使用。

场景 3：在智能金融领域，不同银行和金融机构拥有丰富的客户数据，通过多任务纵向联邦学习，它们可以联合训练模型，以改进欺诈检测任务、信用评分任务和个性化金融服务等任务的准确性和安全性。

20 具体地，任一训练样本对应一个客户（个人或机构），不同银行或金融机构各自持有该客户在本方的交易记录、贷款记录、投资理财记录等。

场景 4：在电子支付领域，参与方是不同的电子钱包，它们可能具有不同的业务类型和服务定位，对风控的侧重点也有所不同。

示例性的，图 1 中的参与方 a 和参与方 b 可以是钱包 A 和钱包 B，钱包 A 的本地数据 a 主要是为商户提供收款和支付服务而产生的业务数据，钱包 B 的本地数据 b 主要是提供个人间的转账和支付服务而产生的业务数据，两个钱包可以协同进行业务数据的学习，从而执行钱包 A 关注的任务 1：欺诈检测任务，以及钱包 B 关注的任务 2：信用评分任务。

以上结合 4 个典型场景，对训练数据在多个参与方中的分布进行示例性介绍。对于训练数据涉及的样本标签，一方面，单个训练样本可能具有 m 个预测任务中任意数量的预测任务下的样本标签。另一方面，样本标签在多个参与方中的分布情况可能有多种，在一种

可能的情况中，各个参与方持有其关注任务对应的样本标签，例如，在上述场景 4 的示例中，钱包 A 持有欺诈检测任务下的样本标签，钱包 B 持有信用评分任务下的样本标签；在另一种可能的情况中，存在部分参与方只有样本特征，没有标签，多任务下的样本标签集中分布在其他参与方中。

5 以上介绍多任务联邦学习场景下，训练数据的具体内容和分布。接下来结合更多附图和实施例，描述上述联邦训练方案的具体实施步骤。

图 2 为本说明书实施例披露的联邦训练方法涉及的中间方和 n 个参与方之间的通信交互示意图。可以理解，中间方一般独立于 n 个参与方，担任这一角色的可以是某个权威机构；中间方和多个参与方中的各方均可以实现为任何具有计算、处理能力的装置、平台、服务器或设备集群等。另外，图 2 中使用 P_i 方指代 n 个参与方中任意的第 i 个参与方。

上述联邦训练方法涉及多轮次迭代训练，如图 2 所示，其中任一轮次的迭代训练包括以下交互步骤：

步骤 S21， P_i 方利用本地模型 w_i 处理对应当前一批次样本的本地特征 x_i ，得到对应的嵌入表征 e_i 。

15 需理解，当前一批次样本是指针对本轮训练采样的一批次样本，一批次样本的数量可以是一个或多个，一般为多个。对于当前一批次样本的确定，有多种方式。比如，由多个参与方中的指定参与方对训练样本的标识集进行针对本轮的随机采样后，将采样出的标识子集发送给其他各方，于是， P_i 方可以定位出标识子集指示的一批次训练样本；又比如，由中间方提前对训练样本标识集进行多次随机采样，并将建立的训练轮次与标识子集的映射表发送给多个参与方，于是， P_i 方可以直接从映射表中读取本轮对应的一批次样本标识。

另外，本地模型 w_i 的结构可以由 P_i 方自行设计选定。示例性的，本地模型 w_i 可以实现为深度学习模型。在首轮迭代训练前， P_i 方可以自行对本地模型 w_i 中的参数进行随机初始化。

25 基于以上， P_i 方可以将上述本地特征 x_i 输入本地模型 w_i ，得到对应的嵌入表征 e_i 。需理解，若当前一批次样本中仅包括一个样本，此时，嵌入表征 e_i 为该样本的表征向量；若当前一批次样本中包括多个样本，此时，嵌入表征 e_i 为该多个样本对应的多个嵌入表征向量而形成的表征矩阵。

由上， P_i 方可以得到当前一批次样本对应的嵌入表征 e_i 。

步骤 S22， P_i 方将嵌入表征 e_i 发送至中间方。

30 步骤 S23，中间方针对 m 个预测任务中任意的第一预测任务 T_j ，利用本地部署的第一

个门控网络 w_j^g 处理从 n 个参与方接收的 n 个嵌入表征 $\{e_i\}_{[n]}$ ，得到 n 个第一权重 $\{\beta_{j_i}\}_{[n]}$ 。

首先需说明，“第一预测任务”、“第一门控网络”中的“第一”，以及文中他处的类似用语，均是为了区分同类事物，不具有排序等其他限定作用。

第一预测任务 T_j 也可以换称为第 j 个预测任务；第一门控网络 w_j^g 中的上标 g 是门控对应的英文单词 gate 的首字母，下标 j 表示其为对应第 j 个预测任务的第 j 个门控网络。示例性的，第一门控网络可以实现为一个或多个全连接网络。

在本步骤中，基于从 n 个参与方接收的 n 个嵌入表征 $\{e_i\}_{[n]}$ ，可以先对其进行融合处理，得到融合表征 e^f 。需理解， $\{e_i\}_{[n]}$ 中的下标 $[n]$ 用于表示 i 的取值是从 1 到 n 的自然数， e^f 的上标 f 是英文单词 fusion 的首字母。示例性的，上述融合处理可以为拼接处理、相加处理或求平均处理，等等。

进一步，可以将融合表征 e^f 输入第一门控网络 w_j^g ，得到 n 个第一权重 $\{\beta_{j_i}\}_{[n]}$ 。可以理解，若当前一批次样本中仅包括一个样本，此时，第一权重为标量；若当前一批次样本中包括多个样本，此时，第一权重为权重向量。另外， $\{\beta_{j_i}\}_{[n]}$ 中的下标 $[n]$ 用于表示 i 的取值是从 1 到 n 的自然数。

由上，中间方可以利用对应 m 个预测任务的 m 个门控网络，得到 n 个嵌入表征 $\{e_i\}_{[n]}$ 在各个预测任务下的一套权重。

步骤 S24，中间方利用 n 个第一权重 $\{\beta_{j_i}\}_{[n]}$ 对 n 个嵌入表征 $\{e_i\}_{[n]}$ 进行加权求和处理，得到第一加权嵌入表征 e'_j 。

对于本步骤中的加权求和处理，可以记作下式：

$$e'_j = \sum_{i=1}^n \beta_{j_i} * e_i \quad (1)$$

由此，可以得到第一预测任务 T_j 对应的第一加权嵌入表征 e'_j ，进而可以得到 m 个预测任务对应的 m 个加权嵌入表征 $\{e'_j\}_{[m]}$ 。需理解， $\{e'_j\}_{[m]}$ 中的下标 $[m]$ 用于表示 j 的取值是从 1 到 m 的自然数。

步骤 S25，中间方利用本地部署的第一预测网络 w_j^s 处理第一加权嵌入表征 e'_j ，得到第一预测结果 $\hat{y}_j$ 。

依此类推，中间方可以得到 m 个预测任务对应的 m 个预测结果 $\{\hat{y}_j\}_{[m]}$ 。示例性的，假定 m 个预测任务包括电子支付领域下的欺诈检测任务和信用评分任务，此时，中间方得到的预测结果可以包括当前一批次样本中各个样本对应的预测欺诈概率和预测守信概率。

需理解， m 个预测结果 $\{\hat{y}_j\}_{[m]}$ 被用于结合对应的 m 份样本标签，进行本轮训练损失 L 的确定。进一步，在一种可能的实施方式中，在执行上述步骤 S25 之后，所述方法还

可以包括以下步骤 S26、S27、S28 和 S29:

在步骤 S26, 中间方基于 m 个预测结果 $\{\hat{y}_j\}_{[m]}$ 和对应的 m 份任务标签 $\{y_j\}_{[m]}$, 确定训练损失 L 。需理解, 中间方持有的 m 份任务标签 $\{y_j\}_{[m]}$ 可以是 n 个参与方提供的。

具体地, 中间方针对所述第一预测任务 T_j , 利用其对应的预测结果 $\hat{y}_j$ 和任务标签 y_j 确定对应的第一任务损失 l_j 。需说明, 计算第一任务损失 l_j 时采用的损失函数可以由中间方自行配置, 也可以由关注第一预测任务 T_j 的参与方, 或者, 由提供第一预测任务 T_j 下样本标签的参与方来决策。

由上, 可以得到 m 个预测任务对应的 m 个任务损失 $\{l_j\}_{[m]}$ 。进一步, 在一个实施例中, 中间方可以对 m 个任务损失 $\{l_j\}_{[m]}$ 进行加权求和, 得到训练损失 L 。对此, 可以记作下式:

$$L = \sum_{j=1}^m \alpha_j * l_j \quad (2)$$

其中, α_j 表示针对第一任务损失 l_j 配置的权重, 为超参数。需理解, α_j 的取值可以由中间方自行设定, 或者, 也可以由 n 个参与方协商决定。

在另一个实施例中, 中间方可以直接将 m 个任务损失 $\{l_j\}_{[m]}$ 的和值确定为训练损失 L 。

另一方面, 还可以在上述训练损失 L 中引入正则项, 以防止模型参数过拟合。

需说明, 在中间方没有获得参与方提供的任务标签的情况下, 中间方需要将 m 个预测结果 $\{\hat{y}_j\}_{[m]}$ 提供给持有对应任务标签的一个或多个参与方, 使得参与方在本地计算第一任务损失 l_j , 于是, 中间方可以根据参与方反馈的 m 个任务损失 $\{l_j\}_{[m]}$, 确定训练损失 L 。

由上, 中间方可以得到当前一批次样本对应 m 个预测任务的训练损失 L 。

步骤 S27, 中间方利用训练损失 L , 更新所述 m 个预测任务下的 m 个预测网络 $\{w_j^s\}_{[m]}$ 和 m 个门控网络 $\{w_j^g\}_{[m]}$, 以及, 计算回传至各个参与方的回传梯度 ∇_i 。

步骤 S28, 中间方将回传梯度 ∇_i 提供给对应的参与方 P_i 。

步骤 S29, 参与方 P_i 利用接收的回传梯度更新本地模型 w_i 。

以上, 在计算出本轮的训练损失 L 后, 可以开启反向传播, 使得中间方和 n 个参与方各自完成本方模型参数的更新, 也就完成了本轮中各模型的迭代更新。

综上, 采用本说明书实施例披露的多任务纵向联邦训练方法, 在参与方不同任务之间共享模型中间结果而不是原始数据, 实现了隐私保护; 同时, 通过共享底层网络结构, 以及为不同任务设置用于聚合中间结果的不同门控网络, 实现了不同任务的数据特征的联合学习和模型参数共享, 从而有效提升了模型的泛化能力, 并减少了训练过程中的通信量。

根据另一方面的实施例, 本说明书实施例还披露一种联合训练装置。图 3 为本说明书

实施例披露的联邦训练装置集成于中间方时的功能结构示意图，其中联合训练涉及中间方和 n 个参与方，所述装置 300 集成于所述中间方，并通过以下模块执行任一轮迭代训练：

嵌入表征接收单元 310，配置为从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到。权重预测单元 320，配置为针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重。结果预测单元 330，配置为利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

在一个实施例中，权重预测单元 320 具体配置为：对所述 n 个嵌入表征进行融合处理，得到融合表征；利用所述第一门控网络处理所述融合表征，得到所述 n 个第一权重。

在一个具体的实施例中，所述融合处理包括拼接处理或相加处理。

在一个实施例中，结果预测单元 330 具体配置为：利用所述 n 个第一权重对所述 n 个嵌入表征进行加权求和，得到所述加权嵌入表征；利用所述第一预测网络处理所述加权嵌入表征，得到所述第一预测结果。

在一个实施例中，所述装置 300 还包括损失确定单元 340，配置为基于所述 m 个预测任务下的 m 个预测结果和对应的 m 个任务标签，确定所述训练损失，用于对各模型进行本轮更新。

进一步，在一个具体的实施例中，损失确定单元 340 具体配置为：针对所述第一预测任务，利用其对应的预测结果和任务标签确定对应的第一任务损失；对所述 m 个预测任务对应的 m 个任务损失进行加权求和，得到所述训练损失。

在一个具体的实施例中，所述第一预测任务对应的任务标签由所述 n 个参与方之一提供，计算所述第一任务损失采用的损失函数由该参与方决策。

在一个具体的实施例中，所述装置 300 还包括：参数更新单元 350，配置为利用所述训练损失，更新所述 m 个预测任务下的 m 个预测网络和 m 个门控网络，以及，计算回传至各个参与方的回传梯度；梯度发送单元 360，配置为将所述回传梯度提供给对应的参与方，使其利用接收的回传梯度更新本地模型。

需理解，为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书时可以把各模块的功能在同一个或多个软件和/或硬件中实现。

The specification also provides a computer-readable non-transitory storage medium, wherein the storage medium stores a computer program, which, when executed by a processor, can be used

to perform one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Herein, the computer-readable non-transitory storage medium or media may include one or more semiconductor-based or other integrated circuits (ICs) (such, as for example, field-programmable gate arrays (FPGAs) or application-specific ICs (ASICs)), hard disk drives (HDDs), hybrid hard drives (HHDs), optical discs, optical disc drives (ODDs), magneto-optical discs, magneto-optical drives, floppy diskettes, floppy disk drives (FDDs), magnetic tapes, solid-state drives (SSDs), RAM-drives, SECURE DIGITAL cards or drives, any other suitable computer-readable non-transitory storage media, or any suitable combination of two or more of these, where appropriate. A computer-readable non-transitory storage medium may be volatile, non-volatile, or a combination of volatile and non-volatile, where appropriate.

The specification also provides a computer system. FIG. 4 illustrates an example computer system 400. In particular embodiments, one or more computer systems 400 perform one or more steps of one or more methods described or illustrated herein. In particular embodiments, one or more computer systems 400 provide functionality described or illustrated herein. In particular embodiments, software running on one or more computer systems 400 performs one or more steps of one or more methods described or illustrated herein or provides functionality described or illustrated herein. Particular embodiments include one or more portions of one or more computer systems 400. Herein, reference to a computer system may encompass a computing device, and vice versa, where appropriate. Moreover, reference to a computer system may encompass one or more computer systems, where appropriate.

This disclosure contemplates any suitable number of computer systems 400. This disclosure contemplates computer system 400 taking any suitable physical form. As example and not by way of limitation, computer system 400 may be an embedded computer system, a system-on-chip (SOC), a single-board computer system (SBC) (such as, for example, a computer-on-module (COM) or system-on-module (SOM)), a desktop computer system, a laptop or notebook computer system, an interactive kiosk, a mainframe, a mesh of computer systems, a mobile telephone, a personal digital assistant (PDA), a server, a tablet computer system, or a combination of two or more of these. Where appropriate, computer system 400 may include one or more computer systems 400; be unitary or distributed; span multiple locations; span multiple machines; span multiple data centers; or reside in a cloud, which may include one or more cloud components in one or more networks. Where appropriate, one or more computer systems 400 may perform without substantial spatial or temporal limitation one or more steps of one or more methods described or illustrated herein. As an example and not by way of limitation, one or more computer

systems 400 may perform in real time or in batch mode one or more steps of one or more methods described or illustrated herein. One or more computer systems 400 may perform at different times or at different locations one or more steps of one or more methods described or illustrated herein, where appropriate.

5 In particular embodiments, computer system 400 includes a processor 402, memory 404, storage 406, an input/output (I/O) interface 408, a communication interface 410, and a bus 412. Although this disclosure describes and illustrates a particular computer system having a particular number of particular components in a particular arrangement, this disclosure contemplates any suitable computer system having any suitable number of any suitable components in any suitable
10 arrangement.

 In particular embodiments, processor 402 includes hardware for executing instructions, such as those making up a computer program. As an example and not by way of limitation, to execute instructions, processor 402 may retrieve (or fetch) the instructions from an internal register, an internal cache, memory 404, or storage 406; decode and execute them; and then write one or more
15 results to an internal register, an internal cache, memory 404, or storage 406. In particular embodiments, processor 402 may include one or more internal caches for data, instructions, or addresses. This disclosure contemplates processor 402 including any suitable number of any suitable internal caches, where appropriate. As an example and not by way of limitation, processor 402 may include one or more instruction caches, one or more data caches, and one or more
20 translation lookaside buffers (TLB s). Instructions in the instruction caches may be copies of instructions in memory 404 or storage 406, and the instruction caches may speed up retrieval of those instructions by processor 402. Data in the data caches may be copies of data of 40 in memory 404 or storage 406 for instructions executing at processor 402 to operate on; the results of previous instructions executed at processor 402 for access by subsequent instructions executing at processor
25 402 or for writing to memory 404 or storage 406; or other suitable data. The data caches may speed up read or write operations by processor 402. The TLBs may speed up virtual-address translation for processor 402. In particular embodiments, processor 402 may include one or more internal registers for data, instructions, or addresses. This disclosure contemplates processor 402 including any suitable number of any suitable internal registers, where appropriate. Where appropriate,
30 processor 402 may include one or more arithmetic logic units (ALUs); be a multi-core processor; or include one or more processors 402. Although this disclosure describes and illustrates a particular processor, this disclosure contemplates any suitable processor.

 In particular embodiments, memory 404 includes main memory for storing instructions for processor 402 to execute or data for processor 402 to operate on. As an example and not by way

of limitation, computer system 400 may load instructions from storage 406 or another source (such as, for example, another computer system 400) to memory 404. Processor 402 may then load the instructions from memory 404 to an internal register or internal cache. To execute the instructions, processor 402 may retrieve the instructions from the internal register or internal cache and decode them. During or after execution of the instructions, processor 402 may write one or more results (which may be intermediate or final results) to the internal register or internal cache. Processor 402 may then write one or more of those results to memory 404. In particular embodiments, processor 402 executes only instructions in one or more internal registers or internal caches or in memory 404 (as opposed to storage 406 or elsewhere) and operates only on data in one or more internal registers or internal caches or in memory 404 (as opposed to storage 406 or elsewhere). One or more memory buses (which may each include an address bus and a data bus) may couple processor 402 to memory 404. Bus 412 may include one or more memory buses, as described below. In particular embodiments, one or more memory management units (MMUs) reside between processor 402 and memory 404 and facilitate accesses to memory 404 requested by processor 402. In particular embodiments, memory 404 includes random access memory (RAM). This RAM may be volatile memory, where appropriate. Where appropriate, this RAM may be dynamic RAM (DRAM) or static RAM (SRAM). Moreover, where appropriate, this RAM may be single-ported or multi-ported RAM. This disclosure contemplates any suitable RAM. Memory 404 may include one or more memories 404, where appropriate. Although this disclosure describes and illustrates particular memory, this disclosure contemplates any suitable memory.

In particular embodiments, storage 406 includes mass storage for data or instructions. As an example and not by way of limitation, storage 406 may include a hard disk drive (HDD), a floppy disk drive, flash memory, an optical disc, a magneto-optical disc, magnetic tape, or a Universal Serial Bus (USB) drive or a combination of two or more of these. Storage 406 may include removable or non-removable (or fixed) media, where appropriate. Storage 406 may be internal or external to computer system 400, where appropriate. In particular embodiments, storage 406 is non-volatile, solid-state memory. In particular embodiments, storage 406 includes read-only memory (ROM). Where appropriate, this ROM may be mask-programmed ROM, programmable ROM (PROM), erasable PROM (EPROM), electrically erasable PROM (EEPROM), electrically alterable ROM (EAROM), or flash memory or a combination of two or more of these. This disclosure contemplates mass storage 406 taking any suitable physical form. Storage 406 may include one or more storage control units facilitating communication between processor 402 and storage 406, where appropriate. Where appropriate, storage 406 may include one or more storages 406. Although this disclosure describes and illustrates particular storage, this disclosure

contemplates any suitable storage.

In particular embodiments, I/O interface 408 includes hardware, software, or both, providing one or more interfaces for communication between computer system 400 and one or more I/O devices. Computer system 400 may include one or more of these I/O devices, where appropriate.

5 One or more of these I/O devices may enable communication between a person and computer system 400. As an example and not by way of limitation, an I/O device may include a keyboard, keypad, microphone, monitor, mouse, printer, scanner, speaker, still camera, stylus, tablet, touch screen, trackball, video camera, another suitable I/O device or a combination of two or more of these. An I/O device may include one or more sensors. This disclosure contemplates any suitable
10 I/O devices and any suitable I/O interfaces 408 for them. Where appropriate, I/O interface 408 may include one or more device or software drivers enabling processor 402 to drive one or more of these I/O devices. I/O interface 408 may include one or more I/O interfaces 408, where appropriate. Although this disclosure describes and illustrates a particular I/O interface, this disclosure contemplates any suitable I/O interface.

15 In particular embodiments, communication interface 410 includes hardware, software, or both providing one or more interfaces for communication (such as, for example, packet-based communication) between computer system 400 and one or more other computer systems 400 or one or more networks. As an example and not by way of limitation, communication interface 410 may include a network interface controller (NIC) or network adapter for communicating with an
20 Ethernet or other wire-based network or a wireless NIC (WNIC) or wireless adapter for communicating with a wireless network, such as a WI-FI network. This disclosure contemplates any suitable network and any suitable communication interface 410 for it. As an example and not by way of limitation, computer system 400 may communicate with an ad hoc network, a personal area network (PAN), a local area network (LAN), a wide area network (WAN), a metropolitan
25 area network (MAN), or one or more portions of the Internet or a combination of two or more of these. One or more portions of one or more of these networks may be wired or wireless. As an example, computer system 400 may communicate with a wireless PAN (WPAN) (such as, for example, a BLUETOOTH WPAN), a WI-FI network, a WI-MAX network, a cellular telephone network (such as, for example, a Global System for Mobile Communications (GSM) network), or
30 other suitable wireless network or a combination of two or more of these. Computer system 400 may include any suitable communication interface 410 for any of these networks, where appropriate. Communication interface 410 may include one or more communication interfaces 410, where appropriate. Although this disclosure describes and illustrates a particular communication interface, this disclosure contemplates any suitable communication interface.

In particular embodiments, bus 412 includes hardware, software, or both coupling components of computer system 400 to each other. As an example and not by way of limitation, bus 412 may include an Accelerated Graphics Port (AGP) or other graphics bus, an Enhanced Industry Standard Architecture (EISA) bus, a front-side bus (FSB), a HYPERTRANSPORT (HT) interconnect, an Industry Standard Architecture (ISA) bus, an INFINIBAND interconnect, a low-pin-count (LPC) bus, a memory bus, a Micro Channel Architecture (MCA) bus, a Peripheral Component Interconnect (PCI) bus, a PCI-Express (PCIe) bus, a serial advanced technology attachment (SATA) bus, a Video Electronics Standards Association local (VLB) bus, or another suitable bus or a combination of two or more of these. Bus 412 may include one or more buses 412, where appropriate. Although this disclosure describes and illustrates a particular bus, this disclosure contemplates any suitable bus or interconnect.

本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。

以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权 利 要 求 书

1. 一种联邦训练方法，涉及中间方和 n 个参与方，所述方法应用于所述中间方，所述方法涉及的任一轮迭代训练包括：

从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；

针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

2. 根据权利要求 1 所述的方法，其中，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重，包括：

对所述 n 个嵌入表征进行融合处理，得到融合表征；

利用所述第一门控网络处理所述融合表征，得到所述 n 个第一权重。

3. 根据权利要求 2 所述的方法，其中，所述融合处理包括拼接处理或相加处理。

4. 根据权利要求 1 所述的方法，其中，利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，包括：

利用所述 n 个第一权重对所述 n 个嵌入表征进行加权求和，得到所述加权嵌入表征；

利用所述第一预测网络处理所述加权嵌入表征，得到所述第一预测结果。

5. 根据权利要求 1 所述的方法，其中，在得到第一预测结果之后，所述方法还包括：基于所述 m 个预测任务下的 m 个预测结果和对应的 m 个任务标签，确定所述训练损失，用于对各模型进行本轮更新。

6. 根据权利要求 5 所述的方法，其中，确定所述训练损失，包括：

针对所述第一预测任务，利用其对应的预测结果和任务标签确定对应的第一任务损失；

对所述 m 个预测任务对应的 m 个任务损失进行加权求和，得到所述训练损失。

7. 根据权利要求 5 所述的方法，其中，所述第一预测任务对应的任务标签由所述 n 个参与方之一提供，计算所述第一任务损失采用的损失函数由该参与方决策。

8. 根据权利要求 5 所述的方法，其中，在确定所述训练损失之后，所述方法还包括：

利用所述训练损失，更新所述 m 个预测任务下的 m 个预测网络和 m 个门控网络，以及，计算回传至各个参与方的回传梯度；

将所述回传梯度提供给对应的参与方，使其利用接收的回传梯度更新本地模型。

9. 一种联邦训练装置，涉及中间方和 n 个参与方，所述装置集成于所述中间方，所述装置通过以下模块执行任一轮迭代训练：

嵌入表征接收单元，配置为从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；

5 权重预测单元，配置为针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；

结果预测单元，配置为利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

10 10. 一种计算机系统，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器集成于中间方，所述中间方和多个参与方协同进行联邦训练；所述处理器执行所述程序时实现任一轮迭代训练中的如下步骤：

从所述 n 个参与方对应接收 n 个嵌入表征，其中各个嵌入表征由对应参与方利用本地模型处理对应当前一批次样本的本地特征而得到；

15 针对 m 个预测任务中任意的第一预测任务，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重；利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，用于确定本轮的训练损失。

11. 根据权利要求 10 所述的计算机系统，其中，利用对应部署的第一门控网络处理所述 n 个嵌入表征，得到 n 个第一权重，包括：

20 对所述 n 个嵌入表征进行融合处理，得到融合表征；

利用所述第一门控网络处理所述融合表征，得到所述 n 个第一权重。

12. 根据权利要求 11 所述的计算机系统，其中，所述融合处理包括拼接处理或相加处理。

25 13. 根据权利要求 10 所述的计算机系统，其中，利用对应部署的第一预测网络处理基于所述 n 个第一权重和 n 个嵌入表征而得到的加权嵌入表征，得到第一预测结果，包括：

利用所述 n 个第一权重对所述 n 个嵌入表征进行加权求和，得到所述加权嵌入表征；

利用所述第一预测网络处理所述加权嵌入表征，得到所述第一预测结果。

14. 根据权利要求 10 所述的计算机系统，其中，在得到第一预测结果之后，所述处理器执行所述程序时还实现如下步骤：

30 基于所述 m 个预测任务下的 m 个预测结果和对应的 m 个任务标签，确定所述训练损失，用于对各模型进行本轮更新。

15. 根据权利要求 14 所述的计算机系统, 其中, 确定所述训练损失, 包括:
针对所述第一预测任务, 利用其对应的预测结果和任务标签确定对应的第一任务损失;
对所述 m 个预测任务对应的 m 个任务损失进行加权求和, 得到所述训练损失。
- 5 16. 根据权利要求 14 所述的计算机系统, 其中, 所述第一预测任务对应的任务标签由
所述 n 个参与方之一提供, 计算所述第一任务损失采用的损失函数由该参与方决策。
17. 根据权利要求 14 所述的计算机系统, 其中, 在确定所述训练损失之后, 所述处理器执行所述程序时还实现如下步骤:
利用所述训练损失, 更新所述 m 个预测任务下的 m 个预测网络和 m 个门控网络, 以及, 计算回传至各个参与方的回传梯度;
- 10 将所述回传梯度提供给对应的参与方, 使其利用接收的回传梯度更新本地模型。
18. 一种计算机可读非易失性存储介质, 其中, 所述存储介质存储有计算机程序, 所述计算机程序被处理器执行时实现上述权利要求 1-8 中任一项所述的方法。