arXiv:2304.08496v1 [cs.SE] 5 Apr 2023

模型驱动量子联邦学习（QFL）

ARMIN MOIN，慕尼黑工业大学和安特卫普大学，armin.moin@tum.de，德国和比利时ATTA BADII，雷丁大学，atta.badii@reading.ac.uk，英国

MOHARRAM CHALLENGER，安特卫普大学和Flanders Make，moharram.challenger@uantwerpen.be，比利时

近期，已有多项研究提出了量子联邦学习（QFL）框架。例如，Google TensorFlow Quantum（TFQ）和 TensorFlow Federated（TFF）库已被用于实现量子联邦学习。然而，开发人员总体而言仍不熟悉量子计算（QC）库和框架。能够为底层量子计算和联邦学习（FL）库提供抽象层的领域专用建模语言（DSML）将大有裨益。借助该语言，从业者可以高效地开展软件开发和数据科学任务，同时部署最先进的量子机器学习（QML）技术。在这篇立场论文中，我们提出扩展现有的、面向机器学习（ML）赋能系统的领域特定模型驱动工程（MDE）工具（如 MontiAnna、ML-Quadrat 和 GreyCat），以支持量子联邦学习。

附加关键词与短语：模型驱动工程、量子计算、联邦机器学习

ACM 参考格式：
Armin Moin、Atta Badii 和 Moharram Challenger。2023。模型驱动量子联邦学习（QFL）。载于 . ACM，纽约州纽约，美国，4 页。https://doi.org/XXXXXXX.XXXXXXX

1 引言与相关工作

联邦学习（FL）提供了一种可扩展且从设计之初就注重隐私保护的机器学习（ML）方法，因为运行学习算法以训练机器学习模型的分布式节点之间不会交换原始数据。因此，在每一轮中，存储机器学习模型参数当前版本的服务器会将这些参数发送给存储机器学习模型训练所需原始数据的分布式节点，这些节点称为客户端。每个节点使用本地数据运行学习算法（例如随机梯度下降（SGD）），并据此更新其本地模型参数。此外，每个客户端会向服务器发送更新后的机器学习模型参数。最后，服务器应用联邦平均[9] 计算新的机器学习模型参数，并将这些参数发送给所有客户端 [4]。

然而，隐私保护并非这种去中心化机器学习方法的唯一优势。相较于传输原始数据，交换机器学习模型参数能够优化网络吞吐量，有助于提升能效，从而减少碳排放足迹。当数据对象包含多变量结构时，这一点尤为明显，例如复杂的高分辨率彩色图像数据，其传输和处理通常会产生更高的能耗和碳排放 [14]。处理具有内在脆弱性的量子数据时，去中心化机器学习的能力变得更加关键，因为这类数据难以传输。需要注意的是，一些适用于量子机器学习（QML）的先进量子计算（QC）技术需要特殊条件，例如极低温度和无振动的

允许出于个人或课堂用途，免费制作本作品全部或部分内容的数字版或纸质副本，前提是不得为盈利或商业利益而制作或分发副本，且副本首页须附有本声明和完整引文。对于本作品中由 ACM 以外的其他方拥有版权的部分，必须尊重其版权。注明出处后可以摘录。除此之外，复制、再版、发布到服务器或分发至列表，均须事先获得特别许可和/或支付费用。请通过 permissions@acm.org 申请许可。© 2023 计算机协会。稿件已提交至 ACM

环境，以存储量子比特并有效维持其量子态 [12]。这使得运行去中心化机器学习的分布式节点之间交换量子数据极其困难且低效，因为量子数据会在与环境相互作用时逐渐衰减 [4, 12]。量子联邦学习（QFL）的优势在于，我们可以在训练机器学习模型的分布式联邦节点（即客户端）上处理内在的量子数据，但仅使用经典（即非量子）数据作为机器学习模型参数，并对其进行交换。

近期，Chehimi和Saad [4] 提出了一个量子联邦学习框架。他们部署了 Google TensorFlow Quantum（TFQ）和 TensorFlow Federated（TFF）库。此外，Yun等人 [15] 提出了 SlimQFL，利用可伸缩神经网络（SNN）支持量子联邦学习，从而应对环境动态，例如时变的通信信道条件和能源限制。然而，大多数软件工程（SE）和数据科学（DS）从业者尚不熟悉量子编程（QP）范式及上述技术。因此，正如文献中的既有工作所强调的，例如 Ali和Yue [3], 、Delgado和Gonzalez [13], 、Gemeinhardt等人 [5], 以及 Moin等人 [11], , 建模语言和模型驱动工程（MDE）范式可能非常适合量子编程，并能带来益处。然而，他们都没有指出支持模型驱动的量子联邦学习的必要性。

2 提议的方法

我们展望未来十年：量子-经典混合应用将部署量子联邦学习技术，以高效应对人工智能解决方案面临的日益严峻挑战。不过，如上所述，目前鲜有从业者（即开发人员和数据科学家）熟悉量子编程，更不用说量子联邦学习了。因此，为了促进量子联邦学习技术在机器学习赋能的软件密集型系统中的部署，我们建议扩展现有的领域特定建模语言和模型驱动工程工具，将其作为支持此类系统开发的赋能技术。这需要增强现有最先进的工具，例如 MontiAnna [8], ML-Quadrat [10], 和 GreyCat [1, 6]，以支持量子联邦学习。

实现所提方法将有助于提高从业者的生产力，缩短新型软件产品和服务的上市时间，并提升软件系统的质量。领域特定建模
已应用于其他领域，并带来了 500% 至 1000% 的生产力跃升 [7]。此外，实现程序合成（即生成源代码以及机器学习模型等其他制品）全面自动化的可能性，可缩短软件产品和服务的开发周期，并通过减少软件缺陷等方式提高软件质量。

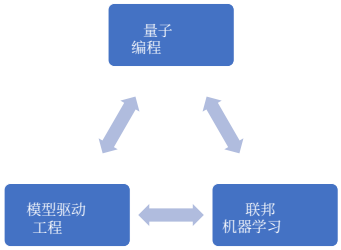

图 1. 所提方法的主要支柱

用于提供上述赋能技术的领域特定建模语言和建模工具，应支持用户（即从业者）在设计时指定参与联邦学习的分布式节点（即客户端和服务器）数量。此外，对于每个节点，还应指定该节点在物理层上是否拥有

量子处理器或经典处理器。此外，还可以提供具体的量子硬件技术（例如超导NISQ与离子阱）以及计算模型（例如量子电路与量子退火）。这有助于针对量子联邦学习应用将要部署的特定量子处理器和经典处理器优化生成的代码。

此外，应能够为参与联邦学习的每个客户端选择首选学习算法、所需的联邦平均算法（例如，适当聚合模型梯度的方法）以及机器学习模型架构。在每种情况下，如果用户（即从业者）未明确提供相应信息，系统应能够自动选择最合适的默认 选项。例如，学习算法、联邦平均算法和机器学习模型架构的默认选项可以分别是随机梯度下降、 [9],的联邦平均算法以及量子卷积神经网络（QCNN） [4], 。

具体而言，我们计划集成基于Cirq [2],的开源TFQ和TFF库，从而以Chehimi和Saad [4]的先前工作为基础。此外，我们打算扩展开源ML-Quadrat项目 [10], ，该项目基于Eclipse建模框架（EMF）和Xtext框架构建。目前，ML-Quadrat既不支持QP，也不支持联邦学习。因此，需要一种能够集成这两项必要功能（即QP和联邦学习，从而实现QFL）的方法。最后，可通过更复杂的QFL解决方案增强领域特定建模语言和工具，例如Yun等人提出的基于SNN的方法 [15]。领域特定建模语言和工具应具备模块化和可扩展性，以支持上述要求。图1展示了所提方法的主要支柱。

3 结论与未来工作

本文提出了实现模型驱动的量子联邦学习的方法。我们指出，现有的领域特定建模语言和建模工具应加以扩展，以满足高级机器学习的需求，尤其是量子联邦学习方面的需求。未来，我们计划实现所提出的解决方案，并开展实验以验证原型。为此，我们将基于现有的量子联邦学习和模型驱动工程解决方案开展工作。

参考文献

[1] 2019. GreyCat：面向大规模动态数据的高效假设分析。*Information Systems* 83（2019年），101–117。[2] n/a。Cirq。https://github.com/quantumlib/Cirq，访问日期：2021-06-24。[3] Shaukat Ali 和 Tao Yue。2020年。量子程序建模：挑战、初步成果与研究方向（*APEQS 2020*）。ACM，纽约州纽约，美国，14–21。[4] Mahdi Chehimi 和 Walid Saad。2022年。基于量子数据的量子联邦学习。载于*IEEE*国际声学、语音与信号处理会议（*ICASSP*）。8617–8621。[5] Felix Gemeinhardt、Antonio Garmendia 和 Manuel Wimmer。2021年。面向模型驱动的量子软件工程。载于第二届量子软件工程国际研讨会（*ICSEW*：*IEEE/ACM*国际软件工程会议研讨会论文集）。[6] T. Hartmann、A. Moawad、F. Fouquet 和 Y. Le Traon。2019年。MDE的下一次演进：将机器学习无缝集成到领域建模中。*Software and System Modeling*（*SoSyM*）18（2019年5月），1285–1304。[7] Steven Kelly 和 Juha-Pekka Tolvanen。2008年。领域特定建模：实现完整代码生成（第1版）。Wiley。[8] Evgeny Kusmenko、Sebastian Nickels、Svetlana Pavlitskaya、Bernhard Rumpe 和 Thomas Timmermanns。2019年。神经处理系统的建模与训练。载于*2019*年 *ACM/IEEE* 第*22*届模型驱动工程语言与系统国际会议（*MODELS*）。283–293。[9] Brendan McMahan、Eider Moore、Daniel Ramage、Seth Hampson 和 Blaise Aguera y Arcas。2017年。基于去中心化数据的深度网络通信高效学习。载于第*20*届人工智能与统计学国际会议论文集（机器学习研究论文集，第*54*卷），Aarti Singh 和 Jerry Zhu（编）。PMLR，1273–1282。[10] Armin Moin、Moharram Challenger、Atta Badii 和 Stephan Günnemann。2022年。面向物联网的机器学习与软件建模的模型驱动方法。*Software and System Modeling*（*SoSyM*）21（2022年），987–1014。[11] Armin Moin、Moharram Challenger、Atta Badii 和 Stephan Günnemann。2022年。面向量子人工智能的模型驱动工程。载于*INFORMATIK2022*，Daniel Demmler、Daniel Krupka 和 Hannes Federrath（编）。1121–1131。[12] Michael A. Nielsen 和 Isaac L. Chuang。2010年。量子计算与量子信息：十周年纪念版。剑桥大学出版社。https://doi.org/10.1017/CBO9780511976667

[13] Carlos A. Pérez-Delgado 和 Hector G. Perez-Gonzalez。2020年。面向量子软件建模语言。载于*IEEE/ACM第42届国际软件工程会议研讨会论文集（大韩民国首尔）（ICSEW'20）*。ACM，纽约州纽约，美国，442–444。[14] Rajkumar K. Raval 和 Atta Badii。2019年。研究图像内容对硬件加速数字空间滤波器能效的影响。24，5（2019年）。[15] Won Joon Yun、Jae Pyoung Kim、Soyi Jung、Jihong Park、Mehdi Bennis 和 Joongheon Kim。2022年。可伸缩量子联邦学习。载于第*39*届国际机器学习会议（*ICML*）上的 *DyNN*（动态神经网络）研讨会，巴尔的摩，马里兰州，美国。