QUANTUM FEDERATIVE LEARNING

EEP55C25 Project Report

Alexandr Goultiaev Tolstokorov
18328823
goultiaa@tcd.ie

January 2023

This report is submitted in part fulfilment for the assessment required in 5C25 Algorithms for Quantum Computing. I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year. These are found in Parts II and III at http://www.tcd.ie/calendar.

Contents

1 Abstract

This report outlines a demonstration of federated learning using a hybrid quantum neural net to classify images of planes and cars from the CIFAR10 dataset. The approach used for the neural net is a hybrid, combining a pre-trained ResNet18 neural network with a quantum variational encoder. The project proves the applicability of federated learning for quantum machine learning and argues for its usefulness in the field.

2 Introduction

With the recent rise in popularity of machine learning (ML) and specifically deep learning (DL) the field has expanded massively to different applications. From speech-recognition[5, 13] and computer vision[14, 19] to finance[8] and playing video and board games[9, 17]. Recently thanks to companies such as IBM, Google, IonQ, D-Wave and software development kits such as Qiskit[18] and Pennylane[1], Quantum is being brought to the public en mass. Quantum computers can theoretically achieve exponential speedup in certain cases that conventional computers struggle with[6]. With this it was no surprise that ML and DL were applied on Quantum Computers with high degree of success rate and sometimes even performing better than their conventional counterparts. However, some applications require access to sensitive data such as medical imaging, text prediction or speech recognition which is to be protected from third parties or bad actors. In conventional ML and DL one of the surging solutions for this challenge is federative learning (FL)[12]. Some research has been conducted in quantum federative computing (QFC) with hybrid conventional-quantum machine learning systems[4] and fully quantum ones[3]. In this report I build and test a hybrid classical-quantum neural network to classify images of automobiles and aeroplanes from the CIFAR10[10] dataset. Then I train the built system in a federated way using a FL framework called Flower[2] and compare it to the conventionally trained network.

2.1 Federated Learning

As outlined before in the Introduction section, FL is an emerging solution to data privacy concerns in large scale deployments of deep learning where sensitive data from many clients is used to train the deep learning model. The main premise of FL is that each client device computes computations and updates to its own local model of the neural network and only sends its weight updates to the central server or body which then uses some strategy to aggregate those updates from the clients and construct the global model. This way no one body has access to the training data and theoretically only the client itself stores its own data with the server only having access to the model updates. The most general FL strategy is called FedAvg and is the one I will be employing in my implementation.

2.1.1 FedAvg

In FedAvg each training round the server will call a subset $\mathcal{C}$ clients out of all the $\mathcal{N}$ clients, these clients will then compute the model updates θ from training with batch size $\mathcal{B}$ for $\mathcal{E}$ epochs. Next the server will average out the θ updates from all the called clients and update its global model which will then send its updated weights to the next $\mathcal{C}$ subset of clients for the next round and repeat that same process.

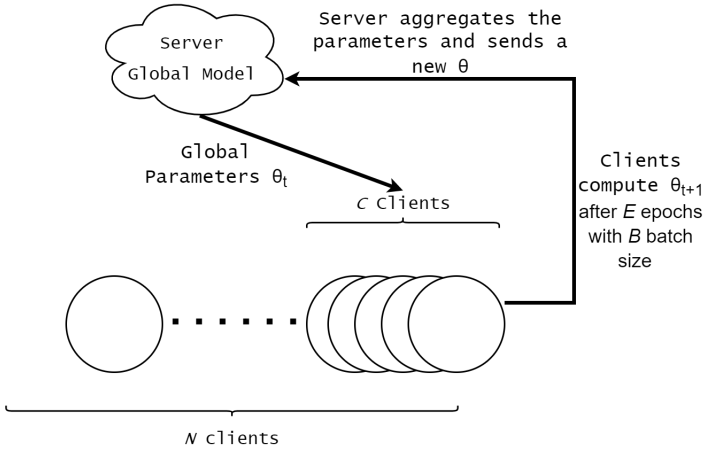


Figure 1: Federated Model.

2.2 Quantum Machine Learning

Quantum neural networks are a special type of quantum circuits with adjustable parameters that can be optimized with machine learning. The most widely implemented circuit for this purpose is a variational quantum circuit (QVC), this circuit consists of an encoding routine of the classical data $E(x)$ followed by a variational circuit block $W(\theta)$ with learnable parameters ϕ.

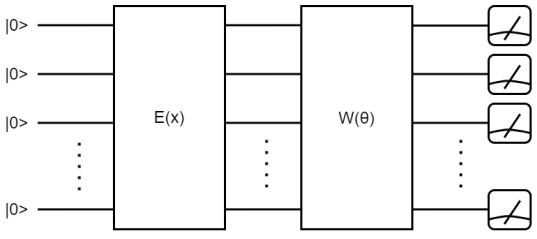
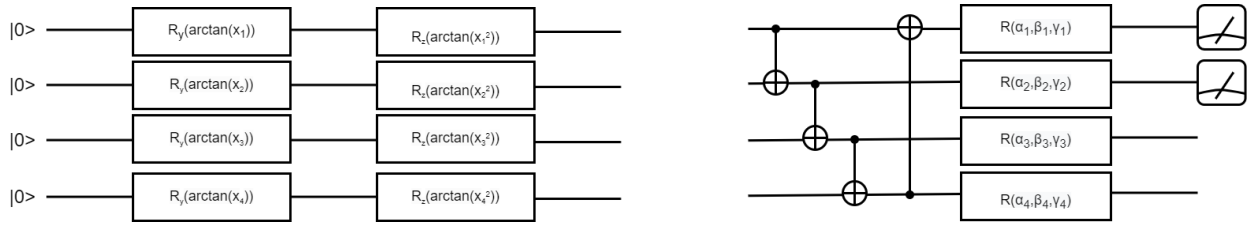


Figure 2: Structure of a variational quantum circuit.

In Figure 3 the QVC that I will be using is shown. The encoder in my QVC consists of a series of single-qubit gates R_y and R_z which are rotations on the y-axis and z-axis respectively.



(a) *Encoder.* ***(b)*** *Variational layer.*

Figure 3: *Encoder and variational layer of a 4-qubit variational quantum classifier.*

These rotation gates depend on the input values x_i and therefore encode the data with respect to the input. The variational layer consists of CNOT gates that entangle each neighbouring pair of qubits and single qubit unitary gates $R(\alpha, \beta, \gamma)$ that have parameters α, β and γ that are subject to iterative optimization. The quantum measurement at the end ill output the Pauli-Z expected values of those qubits, in our case we will be performing binary classification between images of cars or planes so we only measure the first two qubits.

2.2.1 Hybrid Model

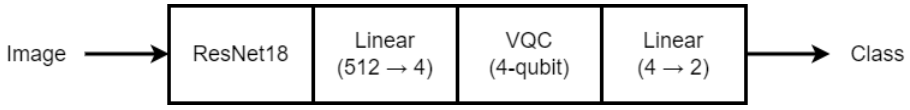


Figure 4: Structure of a hybrid model.

A classical-quantum hybrid model is essentially a classical neural net with some of its layers replaced with a quantum circuit. In my case I am dealing with image classification and thus will use a Convolutional Neural Network (CNN), specifically a pretrained network called ResNet18 [7]. In this CNN the last classifying layers will be replaced by the QVC shown in Figure 3 and the quantum measurement will be the readout of the model. The classical neural net then acts to reduce the tensor of the input image into 4 features as our QVC is 4-qubit.

3 Methodology

The process to build and implement the target hybrid network followed these steps:

I. Build the hybrid neural network following structure shown in Fig4 and using the QVC shown in Fig3.

II. Train and evaluate its performance on the CIFAR10 dataset classifying between planes and cars.

III. Train and evaluate the model in a federated setting using the Flower framework.

Following the outlined structure the hybrid neural network was written using PyTorch[15]. The CIFAR10 dataset had to be filtered as we were interested only in the images belonging to the classes car or plane, this left me with 10 thousand images for training and 2 thousand for testing. Finally the QVC was coded to be 6 deep (i.e. the variational layer in the QVC would repeat 6 times before the readout). These parameters were chosen based on existing implementations of such hybrid networks that demonstrated their effectiveness[11].

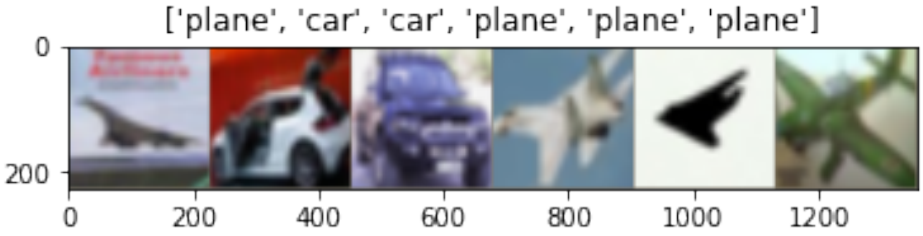


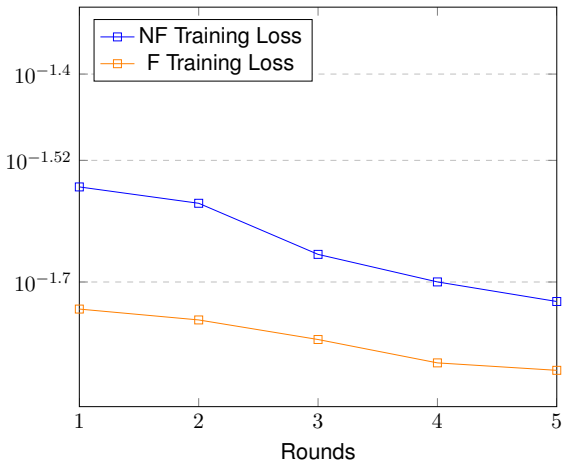
Figure 5: Filtered CIFAR10 dataset sample.

The batch size was set to 32 and the model was trained for 5 epochs. After the model was trained in a federated setting with 10 clients where each round 5 random clients would be called to train the model and the FedAvg strategy was used to compute the global model updates.

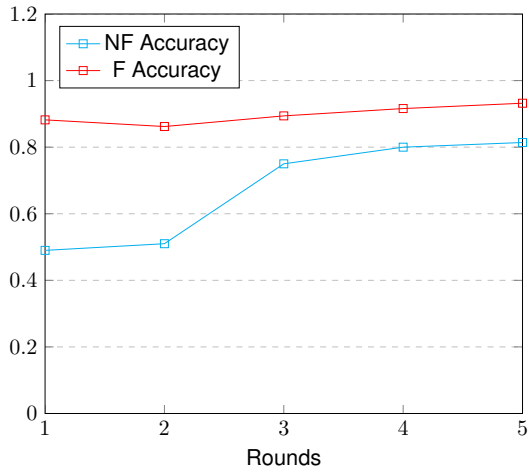
4 Results

Training error and Accuracy					
Model	Epoch 1	Epoch 2	Epoch 3	Epoch 4	Epoch 5
Non-federated Training Loss	0.02745	0.02600	0.02192	0.02000	0.01874
Federated Training Loss	0.01827	0.01762	0.01650	0.01527	0.01489
Non-federated Accuracy	49%	51%	75%	80%	81.4%
Federated Accuracy	88.2%	86.2%	89.4%	91.6%	93.2%

Table 1: *Table of training results.*



(a) *Training Loss plot.*



(b) *Accuracy plot.*

Figure 6: *Plots showing the non-federated NF and the federated F models training results.*

5 Discussion

As shown in the table 1 and the plots from figure 6 the federated model shows an increase of accuracy compared to the non-federated model. However, this apparent better performance is an unfair comparison as each federated round 5 clients compute a training round so in total we end up with 25 computation rounds compared to 5 computation rounds in the non-federated setting. A fairer performance comparison would be to choose the model and training parameters in such a way that the two models compared in computation rounds to properly check convergence speed on both of them.

Nevertheless, federated learning in the context of current quantum computers could be a useful concept when privacy, decentralization and resource limitation is a concern. Right now quantum computation with a large amount of qubits is hard to implement on the so called noisy-intermidiate-scale quantum (NISQ) devices. Therefore federated learning can leverage quantum advantages on NISQ devices and allows us to circumvent some of the limitations. For example, a large array of NISQ devices could be employed to decentralize and improve privacy in certain quantum enhanced DL tasks such as applications in healthcare [16] where privacy is a concern.

Bibliography

[1] BERGHOLM, V., IZAAC, J., SCHULD, M., GOGOLIN, C., ALAM, M. S., AHMED, S., ARRAZOLA, J. M., BLANK, C., DELGADO, A., JAHANGIRI, S., ET AL. Pennylane: Automatic differentiation of hybrid quantum-classical computations. *arXiv preprint arXiv:1811.04968* (2018).

[2] BEUTEL, D. J., TOPAL, T., MATHUR, A., QIU, X., PARCOLLET, T., DE GUSMÃO, P. P., AND LANE, N. D. Flower: A friendly federated learning research framework. *arXiv preprint arXiv:2007.14390* (2020).

[3] CHEHIMI, M., AND SAAD, W. Quantum federated learning with quantum data. In *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2022), IEEE, pp. 8617–8621.

[4] CHEN, S. Y.-C., AND YOO, S. Federated quantum machine learning. *Entropy 23*, 4 (2021), 460.

[5] DENG, L., HINTON, G., AND KINGSBURY, B. New types of deep neural network learning for speech recognition and related applications: an overview. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing* (2013), pp. 8599–8603.

[6] HARROW, A. W., AND MONTANARO, A. Quantum computational supremacy. *Nature 549*, 7671 (2017), 203–209.

[7] HE, K., ZHANG, X., REN, S., AND SUN, J. Deep residual learning for image recognition, 2015.

[8] HEATON, J., POLSON, N. G., AND WITTE, J. H. Deep learning in finance. *arXiv preprint arXiv:1602.06561* (2016).

[9] JUSTESEN, N., BONTRAGER, P., TOGELIUS, J., AND RISI, S. Deep learning for video game playing. *IEEE Transactions on Games 12*, 1 (2019), 1–20.

[10] KRIZHEVSKY, A., HINTON, G., ET AL. Learning multiple layers of features from tiny images.

[11] MARI, A., BROMLEY, T. R., IZAAC, J., SCHULD, M., AND KILLORAN, N. Transfer learning in hybrid classical-quantum neural networks. *Quantum 4* (2020), 340.

[12] MCMAHAN, B., MOORE, E., RAMAGE, D., HAMPSON, S., AND Y ARCAS, B. A. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics* (2017), PMLR, pp. 1273–1282.

[13] NASSIF, A. B., SHAHIN, I., ATTILI, I., AZZEH, M., AND SHAALAN, K. Speech recognition using deep neural networks: A systematic review. *IEEE access 7* (2019), 19143–19165.

[14] O'MAHONY, N., CAMPBELL, S., CARVALHO, A., HARAPANAHALLI, S., HERNANDEZ, G. V., KRPALKOVA, L., RIORDAN, D., AND WALSH, J. Deep learning vs. traditional computer vision. In *Science and information conference* (2019), Springer, pp. 128–144.

[15] PASZKE, A., GROSS, S., MASSA, F., LERER, A., BRADBURY, J., CHANAN, G., KILLEEN, T., LIN, Z., GIMELSHEIN, N., ANTIGA, L., DESMAISON, A., KOPF, A., YANG, E., DEVITO, Z., RAISON, M., TEJANI, A., CHILAMKURTHY, S., STEINER, B., FANG, L., BAI, J., AND CHINTALA, S. Pytorch: An imperative style, high-performance deep learning library. In *Advances in Neural Information Processing Systems 32*. Curran Associates, Inc., 2019, pp. 8024–8035.

[16] SIERRA-SOSA, D., ARCILA-MORENO, J., GARCIA-ZAPIRAIN, B., CASTILLO-OLEA, C., AND ELMAGHRABY, A. Dementia prediction applying variational quantum classifier, 2020.

[17] SILVER, D., HUANG, A., MADDISON, C. J., GUEZ, A., SIFRE, L., VAN DEN DRIESSCHE, G., SCHRITTWIESER, J., ANTONOGLOU, I., PANNEERSHELVAM, V., LANCTOT, M., ET AL. Mastering the game of go with deep neural networks and tree search. *nature 529*, 7587 (2016), 484–489.

[18] TA V, A., ANIS, M. S., ABBY-MITCHELL, ABRAHAM, H., ADUOFFEI, AGARWAL, R., AGLIARDI, G., AHARONI, M., AJITH, V., AKHALWAYA, I. Y., ALEKSANDROWICZ, G., AND MANY OTHERS. Qiskit: An open-source framework for quantum computing, 2021.

[19] VOULODIMOS, A., DOULAMIS, N., DOULAMIS, A., AND PROTOPAPADAKIS, E. Deep learning for computer vision: A brief review. *Computational intelligence and neuroscience 2018* (2018).