

TRAINING SPEECH RECOGNITION MODELS WITH FEDERATED LEARNING: A QUALITY/COST FRAMEWORK

Dhruv Guliani

Françoise Beaufays

Giovanni Motta

Google, Mountain View, CA, U.S.A
dguliani@google.com

ABSTRACT

We propose using federated learning, a decentralized on-device learning paradigm, to train speech recognition models. By performing epochs of training on a per-user basis, federated learning must incur the cost of dealing with non-IID data distributions, which are expected to negatively affect the quality of the trained model. We propose a framework by which the degree of non-IID-ness can be varied, consequently illustrating a trade-off between model quality and the computational cost of federated training, which we capture through a novel metric. Finally, we demonstrate that hyperparameter optimization and appropriate use of variational noise are sufficient to compensate for the quality impact of non-IID distributions, while decreasing the cost.

Index Terms— speech recognition, federated learning.

1. INTRODUCTION

The increasing ubiquity of mobile devices with high computational power [1], along with advances in sequence-to-sequence neural networks [2, 3], have made it possible to develop mobile applications powered by on-device automatic speech recognition (ASR) systems [4]. For example, neural ASR models with state-of-the-art quality [5] have been deployed on-device with additional latency and reliability benefits [6] relative to server-based models.

Considering user privacy in the context of on-device ASR, we investigate the feasibility of training speech models on-device using federated learning (FL) [7, 8]. FL is a decentralized training method that does not require sending raw user data to central servers. Instead, user data are stored in an on-device *training cache*, where training iterations can be performed. FL optimization proceeds in synchronous *rounds* of training, wherein a set of *clients* (devices) contributes updates to a central model. FL has been successfully deployed in large production systems to perform emoji prediction [9], next-word prediction [10], and query suggestion [11].

When used to perform per-user training of models, FL presents an inherent difference in comparison to centralized training in that training data under FL are non-IID. With standard central mini-batch training, an IID (independent

and identically distributed) assumption is typically made as examples are sampled with a uniform probability across the training set. Under FL, examples are sampled from client distributions which may be similar, but not identical (non-IID). Training on non-IID data has been shown to be sub-optimal across multiple domains [12, 13, 14] and remains an open problem in federated learning [15, 16].

In this work, we study the impact of speaker-split (non-IID) data in the context of ASR training, and make the following contributions:

- We provide a mental model to reason about the differences between IID and non-IID training.
- We introduce a general *cost* function for FL which measures the computational cost of model quality.
- We show that ASR models trained with FL can achieve the same quality as server-trained models.

2. METHODOLOGY

2.1. Federated Averaging Algorithm

A common optimization algorithm for FL is Federated Averaging (*FedAvg*) [7]. Outlined in Algorithm 1, *FedAvg* consists of two levels of optimization: local optimization performed on K participating clients, and a server step to update the global model. *FedAvg* is used in all experiments in this work.

Algorithm 1 *FedAvg*. The K clients are indexed by k , rounds are indexed by r , and n is the number of examples.

```

1: initialize  $w^0$ 
2: for each round  $r = 1, 2, \dots$  do
3:    $K \leftarrow$  (random subset of  $M$  clients)
4:   for each client  $k \in K$  in parallel do
5:      $\hat{w}_k^r \leftarrow \text{ClientUpdate}(k, w^r)$ 
6:      $\Delta w_k^r = w^r - \hat{w}_k^r$ 
7:   end for
8:    $\bar{w}^r = \sum_{k=1}^K \frac{n_k}{n} \Delta w_k^r$  ▷ Weighted average
9:    $w^{r+1} = w^r - \eta \bar{w}^r$  ▷ Server update
10: end for

```

2.2. Understanding non-IID Data

对于non-IID数据，DL训练出来的model 也会下降

Various studies have shown noticeable quality degradation when training neural models with non-IID data. Strategies to mitigate this include accounting for client model drift [14], using adaptive optimizers [17], tuning local optimization hyper-parameters [12, 7], and weighting client updates with estimates of client data skew [16, 18, 19].

In this work, we build on the observation that, given an increased computation budget, a non-IID distribution can be modified to approximate an IID one. To elaborate, in a federated training round, a set of clients is randomly selected from a training population. If, in the client optimization, a single local example is sampled and used to compute an SGD update with learning rate 1, raw gradients would be aggregated in the server update step. As the sampling of clients in a federated training round is random, the server step would aggregate effectively IID contributions in this example. However, training in this manner would likely cause a sharp increase in the number of rounds needed for convergence, and subsequently increase training time and server-client communication.

We therefore note that the degree of non-IID-ness in a particular experiment can be varied at the expense of computational cost, and this idea can be used to make adjustments to the experimental setup depending on the desired quality-performance trade-off.

2.3. The Cost of Federated Model Quality

联邦学习的质量

We capture the cost of federated computation through a metric we name the *Cost of Federated Model Quality (CFMQ)*. This is, to our knowledge, the first attempt at formulating a general cost function which may be adapted for any federated optimization. Along with non-IID/IID considerations, this cost function helps compare the impact of convergence time, local optimization, client participation and communication payload on quality. Therefore, when used in conjunction with a quality metric, the CFMQ provides a useful way to compare experiments. 质量度量+CFMQ联合

Let μ be the average number of local optimization steps taken by a client. Let e be the number of local epochs, N the total number of examples in a round, b the batch size, and K the number of clients participating. It follows that:

$$\mu = \frac{eN}{bK} \quad (1)$$

Let P be the round-trip communication payload in bytes, R the number of rounds, and ν the peak memory consumed during a step. Equation 2 unifies the communication cost and local computation cost, as these are the two resource-constrained aspects of the federated optimization [11]. We assume an abundance of server resources/memory in our study. We therefore formulate the cost CFMQ as:

$$\text{CFMQ} = RK(P + \alpha\mu\nu) \quad [\text{bytes}] \quad (2)$$

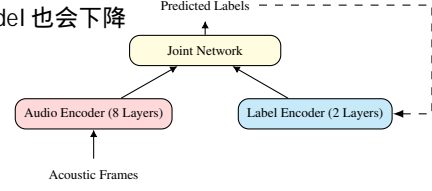


Fig. 1. RNN-T speech model architecture.

α is a balancing term added to the CFMQ, and can be modified to adjust the importance of the two components of cost.

3. MODEL AND DATA

3.1. Model Architecture

We use the RNN-T architecture [5] depicted in Figure 1 in this paper. The model has 122M trainable parameters, and predicts the probability $P(y|x)$ of labels y given acoustic data x . It consists of an LSTM audio encoder, an LSTM label encoder, a fully-connected layer concatenating the encoder outputs, and an output softmax. The input acoustic frames are 128-dimensional log-mel filterbank energies, and output labels belong to a set of 4096 word-pieces.

3.2. Librispeech Corpus

We use the Librispeech [20] corpus, containing 960 hours of transcribed training utterances from 2338 speakers, and 21 hours of evaluation audio from 146 speakers split amongst 4 sets *Dev*, *DevOther*, *Test*, and *TestOther*, with the reporting metric of *Word Error Rate (WER)*. The sets labelled “Other” are intended to be more difficult to recognize. The data are evenly balanced in terms of male and female speakers.

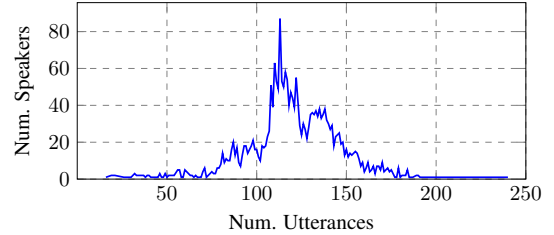


Fig. 2. Histogram of utterance distribution across speakers.

We run FL experiments on this corpus by associating each speaker label to a device that could participate in rounds of federated training. Librispeech data, when split by speaker, are non-IID for a variety of reasons including differences in voice, vocabulary, recording quality, and utterance counts (as represented in Figure 2) across users.

4. EXPERIMENTS

4.1. Baseline and Federated Training

We conducted a series of experiments to recover quality degradation due to non-IID training, and compared them to a centrally trained IID Baseline. The Baseline configuration was trained with a linear ramp-up learning rate schedule, SpecAugment [21], and Variational Noise [22]. Baseline results (*E0*) can be found in Table 1.

Federated training of RNN-T models was performed using *FedAvg* on a FL simulator written in TensorFlow [23] running on TPU [24] hardware, where data were split by speaker. Training hyper-parameters were kept as similar to the Baseline as possible, with the exception of Variational Noise initially being omitted as it needed to be adapted for the FL (discussed further in 4.2.2).

4.2. Matching Baseline Model Quality

In non-IID federated experiments, *SGD* was used as the client optimizer with a constant learning rate which was set to 0.008 through a coarse sweep. Adam [17] was used for the server update. The number of participating clients, K , was gradually increased from 32 to 128, beyond which it stopped offering improvements to model quality. In this configuration, clients cycled through local data over a single epoch. Table 1 shows

ID	Exp.	WER			
		Test	TestOther	Dev	DevOther
E0	Baseline	4.8	12.1	5.1	12.1
E1	Non-IID	6.8	17.2	7.0	17.3
<i>E0 v. E1 % Rel. WER</i>		+42%	+42%	+37%	+43%

Table 1. Quality degradation with non-IID training.

the Baseline performance and the initial non-IID config, with a substantial WER degradation across all evaluation sets.

4.2.1. Limiting Per-speaker Data

In an attempt to push data distributions closer to IID and minimize per-client drift, a subset of examples were randomly sampled from each speaker participating in a federated round to impose a per-client data limit. We show that data-limiting pushes distributions to be more IID through a thought experiment, wherein a single example is sampled from each client. In this scenario, assuming client-selection is random, the participating data in a round is as close as possible to IID.

It is important to note that the entire per-speaker dataset was still seen over the course of multiple rounds.

Table 2 illustrates the quality improvement due to data-limiting, bringing WER degradation from over 40% to less than 30% relative across all sets.

ID	Data Limit	WER			
		Test	TestOther	Dev	DevOther
E1	None	6.8	17.2	7.0	17.3
E2	32	6.2	14.8	6.5	15.3
E3	64	6.5	15.1	6.8	15.5
E4	128	7.1	16.4	7.1	16.5
<i>E0 v. E2 % Rel. WER</i>		+29%	+22%	+27%	+26%

Table 2. Impact of data-limiting on non-IID training.

4.2.2. Federated Variational Noise

The Baseline used Variational Noise [22] (VN), applied by adding Gaussian noise to model parameters during each optimization step. A modification had to be made to VN in order to accommodate the two-step optimization that exists in FL: allowing each client to add its own random noise tensors during local optimization. We called this *Federated Variational Noise* (FVN), and found it was critical to recuperating the non-IID quality degradation. Table 3 shows experiments *E5* and *E6*, which introduced FVN in a similar manner to the Baseline. We exceeded Baseline model quality by further improving the application of FVN in *E7*, wherein we increased the standard deviation of Gaussian noise linearly during training.

ID	FVN Std Dev	WER			
		Test	TestOther	Dev	DevOther
E2	-	6.2	14.8	6.5	15.3
E5	0.01	5.1	12.6	5.5	12.4
E6	0.02	5.0	12.2	5.2	12.4
E7	Ramp to 0.03	4.6	11.9	5.0	11.9
<i>E0 v. E7 % Rel. WER</i>		-4%	-2%	-2%	-2%

Table 3. Impact of FVN on non-IID training.

In addition, we hypothesize that FVN regularizes non-IID client drift because VN was designed to reduce entropy in Bayesian inference tasks. It is based on the idea that model parameters are like random variables sampled from a prior distribution, γ , which can be better approximated with a given distribution $Q(\beta)$ by adding Gaussian noise during training. Therefore, under FL, if noise from the same underlying Gaussian is applied on each client, the resulting approximation is that all client model parameters are sampled from the same $Q(\beta)$ distribution, thus limiting per-client drift.

Results in Table 2 show that model quality degrades as the per-client data volume is increased. Client models *drift* in varying directions, causing server updates to be sub-optimal. However, experiments *E7* and *E8* in Table 4 show that, with the addition of FVN, there is minimal change in model quality even without per-client data limits. This adds evidence to our claim that FVN prevents client drift.

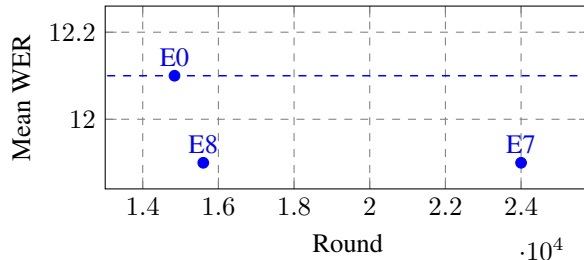
ID	Data Limit	WER			
		Test	TestOther	Dev	DevOther
E7	32	4.6	11.9	5.0	11.9
E8	-	4.6	11.9	5.1	11.8

Table 4. Impact of data-limiting on FVN experiments.

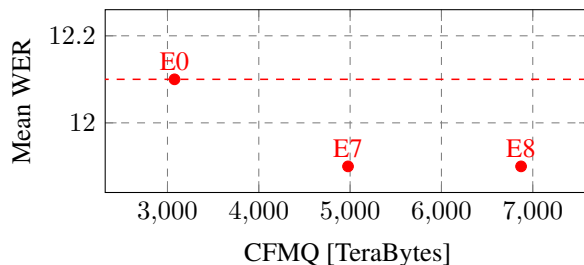
4.3. Computational Efficiency

4.3.1. Quality-Cost Analysis

So far, we focused on quality impact due to non-IID training. However, as described in Section 2.3, a crucial aspect of designing an FL system lies in its computational cost. In production FL, model payload size would vary per-experiment due to the presence of transport compression. Likewise, client memory usage would vary across devices due to differing hardware characteristics. Motivated by simplicity, approximations were used in this analysis. The round trip communication payload was approximated to be twice the model size (960 MB), and peak memory was approximated as the size of the model plus 10% intermediate storage (660 MB). As Eq. 2 also requires α to be set, it was chosen as 1 for this study.



(a) Comparing experiments by rounds to convergence.



(b) Comparing experiments by cost function.

Fig. 3. Experiment efficiency comparison.

Figure 3 shows the quality-cost trade-off for key experiments from the previous section, contrasting number of rounds as the measure of cost against CFMQ. Quality is measured through mean WER on the *Other* evaluation sets, as these are more challenging. If rounds to convergence is the measure of cost, *E8* achieved better quality than the Baseline for a marginal increase in cost. However, when using CFMQ,

it is clear that *E7* achieved the same quality as *E8* at lower cost. This is due to the fact that no per-client data limits were imposed in *E8*, leading clients to take more local optimization steps than in *E7* for the same model quality.

4.3.2. Reducing the Cost of non-IID Model Quality

Experiments thus far have recuperated the quality loss due to non-IID training data, but incurred an increase in cost. New experiments, aimed at reducing cost, were conducted by varying the number of local epochs, server learning rate schedule, and amount of SpecAugment. Table 5 shows the two most promising experiments, *E9* and *E10*, which had a lower CFMQ and better quality in comparison to the Baseline. They both modified the learning rate schedule to have a shorter ramp-up and introduced an exponential decay. *E10* increased the amount of SpecAugment during the training procedure and yielded slightly better quality. Therefore, we were able to recuperate the quality degradation from non-IID training data at a lower computation cost than the IID Baseline in this study. We must note that in order to limit scope we did not re-visit and refine the Baseline in this work.

ID	CFMQ [TB]	WER			
		Test	TestOther	Dev	DevOther
E0	3077	4.8	12.1	5.1	12.1
E9	2779	4.8	11.4	4.6	11.5
E10	2945	4.8	11.4	4.6	11.4

Table 5. Exceeding Baseline quality with lower CFMQ.

5. CONCLUSION

Federated learning implies training on non-IID data, a property that has been considered a potential drawback of the technique. We argued that the degree of non-IID-ness can be adjusted through random client data sampling, resulting in a flexible cost-quality trade-off. Initially, recuperating quality in a federated setting is likely to lead to a cost increase. When this is resolved, e.g. through optimizer configuration, hyperparameter tuning, and use of regularizers, FL can provide IID-level quality at relatively low costs. We demonstrated that this double optimization could be performed for the federated learning of a state-of-the-art ASR model, resulting in a better model at lower cost than the baseline Adam-SGD model.

6. ACKNOWLEDGEMENTS

We would like to thank Khe Chai Sim, Lillian Zhou, Petr Zadrazil, Hang Qi, Harry Zhang, Yuxin Ding, and Tien-Ju Yang for providing valuable insights on its structure and contents.

7. REFERENCES

- [1] “Mobile Fact Sheet: Mobile Phone Ownership Over Time,” <https://www.pewresearch.org/internet/fact-sheet/mobile/>, 2019, Accessed: 2020-09-22.
- [2] A. Graves, “Sequence Transduction with Recurrent Neural Networks,” *CoRR*, vol. abs/1211.3711, 2012.
- [3] A. Graves, A. Mohamed, and G. Hinton, “Speech Recognition with Deep Recurrent Neural Networks,” in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 6645–6649.
- [4] T. N. Sainath, Y. He, B. Li, and other, “A Streaming On-Device End-To-End Model Surpassing Server-Side Conventional Model Quality and Latency,” 05 2020, pp. 6059–6063.
- [5] Y. He, T. N. Sainath, R. Prabhavalkar, et al., “Streaming End-to-end Speech Recognition for Mobile Devices,” in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 6381–6385.
- [6] Google Inc., “An All-Neural On-Device Speech Recognizer,” <https://ai.googleblog.com/2019/03/an-all-neural-on-device-speech.html>, 2019, Accessed: 2020-10-08.
- [7] H. B. McMahan, E. Moore, et al., “Communication-Efficient Learning of Deep Networks from Decentralized Data,” in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 20-22 April 2017, Fort Lauderdale, FL, USA*, A. Singh and X. (Jerry) Zhu, Eds. 2017, vol. 54 of *Proceedings of Machine Learning Research*, pp. 1273–1282, PMLR.
- [8] K. Bonawitz, H. Eichner, et al., “Towards Federated Learning at Scale: System Design,” in *SysML 2019*, 2019, To appear.
- [9] F. Beaufays, K. Rao, R. Mathews, et al., “Federated Learning for Emoji Prediction in a Mobile Keyboard,” 2019.
- [10] A. Hard, K. Rao, R. Mathews, et al., “Federated Learning for Mobile Keyboard Prediction,” *CoRR*, vol. abs/1811.03604, 2018.
- [11] T. Yang, G. Andrew, H. Eichner, et al., “Applied Federated Learning: Improving Google Keyboard Query Suggestions,” *CoRR*, vol. abs/1812.02903, 2018.
- [12] T. H. Hsu, H. Qi, and M. Brown, “Measuring the Effects of Non-Identical Data Distribution for Federated Visual Classification,” *CoRR*, vol. abs/1909.06335, 2019.
- [13] A. Hard, K. Partridge, C. Nguyen, et al., “Training Keyword Spotting Models on Non-IID Data with Federated Learning,” 2020.
- [14] Y. Zhao, M. Li, L. Lai, et al., “Federated Learning with Non-IID Data,” *CoRR*, vol. abs/1806.00582, 2018.
- [15] P. Kairouz, H. B. McMahan, et al., “Advances and Open Problems in Federated Learning,” 2019.
- [16] K. Hsieh, A. Phanishayee, O. Mutlu, et al., “The Non-IID Data Quagmire of Decentralized Machine Learning,” 2019.
- [17] S. Reddi, Z. Charles, M. Zaheer, et al., “Adaptive Federated Optimization,” 2020.
- [18] D. Dimitriadis, K. Kumatani, R. Gmyr, et al., “Federated Transfer Learning with Dynamic Gradient Aggregation,” 2020.
- [19] T. H. Hsu, H. Qi, and M. Brown, “Federated Visual Classification with Real-World Data Distribution,” 2020.
- [20] V. Panayotov, G. Chen, D. Povey, and S. Khudanpur, “Librispeech: An ASR Corpus Based on Public Domain Audio Books,” in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2015, pp. 5206–5210.
- [21] D. S. Park, W. Chan, Y. Zhang, et al., “SpecAugment: A Simple Data Augmentation Method for Automatic Speech Recognition,” *Interspeech 2019*, Sep 2019.
- [22] A. Graves, “Practical Variational Inference for Neural Networks,” in *Advances in Neural Information Processing Systems 24*, J. Shawe-Taylor, R. S. Zemel, P. L. Bartlett, et al., Eds., pp. 2348–2356. Curran Associates, Inc., 2011.
- [23] M. Abadi, P. Barham, , J. Chen, et al., “TensorFlow: A System for Large-scale Machine Learning,” in *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, 2016, pp. 265–283.
- [24] N. P. Jouppi, C. Young, et al., “In-datacenter Performance Analysis of a Tensor Processing Unit,” in *2017 ACM/IEEE 44th Annual International Symposium on Computer Architecture (ISCA)*, 2017, pp. 1–12.