Contextual Model Aggregation for Fast and Robust Federated Learning in Edge Computing

Hung T. Nguyen*, H. Vincent Poor*, and Mung Chiang†,
*Princeton University, {hn4,poor}@princeton.edu
†Purdue University, chiang@purdue.edu

Abstract—Federated learning is a prime candidate for distributed machine learning at the network edge due to the low communication complexity and privacy protection among other attractive properties. However, existing algorithms face issues with slow convergence and/or robustness of performance due to the considerable heterogeneity of data distribution, computation and communication capability at the edge. In this work, we tackle both of these issues by focusing on the key component of model aggregation in federated learning systems and studying optimal algorithms to perform this task. Particularly, we propose a contextual aggregation scheme that achieves the optimal context-dependent bound on loss reduction in each round of optimization. The aforementioned context-dependent bound is derived from the contextual aggregation and show robust performance even in the most extreme settings.

Index Terms—Federated learning, distributed optimization, robust learning, edge computing systems

I. INTRODUCTION

Federated learning (FL) was first introduced in [1] as a distributed machine learning algorithm and has been largely accepted as a framework of choice in edge learning systems due to the numerous nice properties including low communication complexity and data privacy protection, which has been in the spotlight in recent years. This coupled with the explosive increases of smart devices, e.g., smartphones, wearables, autonomous vehicles, in both number and capability, has fueled substantial research efforts [2]–[4] to understand and develop FL algorithms with better convergence properties and higher adaptivity to the inherent heterogeneity in edge learning systems. It is also on the same line with the recent trend of migrating from cloud to edge for better latency and improving user experience.

The FL framework assumes a network of $N$ connected heterogeneous devices, each of which owns a separate set of private local data and wishes to learn a machine learning model collaboratively with other devices without sharing any data. In addition, there is a central server that can communicate, aggregate and exchange model parameters with all the devices. A typical FL algorithm unfolds in multiple rounds, and in each round $t$, a small set $S_t$ of $K$ random devices are selected to perform local optimization from the current parameters and send updates to the central server for aggregation. The newly aggregated parameters form the latest model and will be updated upon in the next round. Figure 1 illustrates the components of FL framework and the focus of our work. We can identify multiple inherent sources of heterogeneity in this framework: 1) (statistical) non-i.i.d. data across devices; 2) (system) different computing resources at devices; and 3) (system) varying communication latency between central server and devices. Thus, on top of challenges in traditional distributed optimization in the cloud, we need to address issues associated with the inherent heterogeneity in FL setting.

FedAvg [1] was the first FL algorithm and has demonstrated outstanding performance in different tasks, however, its performance degrades greatly in heterogeneous environments, and much development has been made to analyze and improve the convergence rate of FedAvg [5]–[11]. Most of these works focus on modifying local optimizers to mitigate data heterogeneity and prove promising convergence rates under assumptions on smoothness, bounded dissimilarity between data distribution across devices, and/or function convexity. Most notably, FedProx [8] incorporates a proximal term in each local loss function to penalize drastic changes of parameters in each round and, therefore, prevent majorly conflicting updates from devices with totally different data. Very recently, FOLB
[11] focuses on the aggregation scheme at the central server and integrates a weighted averaging by inner product between local and global gradients. However, as shown in [8], [11], although recent methods provide better performance than FedAvg, they struggle with keeping the results robust throughout the optimization process and experience wide fluctuations, even in consecutive rounds.

In this work, we aim at addressing both convergence and robustness issues in federated learning by studying optimal aggregation algorithms at the central server. Given the inherent heterogeneity at multiple scales, the aggregation step is the key to distilling local updates from selected devices and forming a robust model parameters. We consider a general form of model aggregation and derive a context-dependent bound based on the particular set of selected devices, referred to as context of that round hereafter, and a minimal assumption of the overall loss function being smooth (common in both convex and non-convex optimizations). Then, the optimal setting of model aggregation is derived by optimizing the context-dependent bound and is used to form the next global model parameters. We prove a definite reduction off the loss function with the magnitude depending on the local updates and aggregation variables derived by our technique. We also study the bound in expectation over all random choices of participants and derive a corresponding aggregation.

In the experiments, we consider multiple variants of our aggregation, which differ in hyper-parameter settings, and show consistently high performance and robustness between variants. We also integrate the contextual aggregation scheme with existing FL algorithms and reveal significant improvements in terms of convergence speed and much better robustness property. The contextual versions can reduce the number of optimization rounds to achieve the same accuracy levels effectively by a factor of three or more across various settings and datasets. We summarize our contributions as follows:

- We study a general form of model aggregation at the central server in federated learning and propose an optimal aggregation in a general form to optimize a context-dependent bound based on the specific participating devices in each round. The context-dependent bound only relies on the particular set of devices and a minimal smoothness assumption of the overall loss function.
- We show that the proposed contextual aggregation results in definite loss reduction with the magnitude depending on local updates. We extend our scheme to the case of optimizing the expected loss reduction over random device selection.
- We examine variants of the contextual aggregation and perform extensive experiments in various settings and datasets to demonstrate faster convergence and much higher robustness when integrating the new scheme into existing federated learning algorithms.

II. PRELIMINARIES

We introduce the system model (Subsection II-A), different types of heterogeneity (Subsection II-B), and details of important federated learning algorithms (Subsection II-C) that we consider most related and compare with throughout this work.

A. System models and problem definition

We consider a network of $N$ devices, indexed from 1 to $N$. Each device $k$ contains a private dataset $D_k$ and each data point $d \in D_k$ is a pair of feature vector $x_d$ and label $y_d$ (in classification or regression task). Additionally, there is a central server that is connected with all $N$ devices. The problem of interest is to learn a common machine learning model collaboratively using all the available data in the entire network without sharing any (private) data. In other words, the common model works well on all the devices and achieves better generalization than one trained on a single local dataset. We also wish to incur minimal communication between devices and server to avoid interfering with network operations.

More specifically, the machine learning model is identified by a parameter vector $w$ in $n$-dimensional space and a loss function $f(w) = \frac{1}{|\mathcal{D}|} \sum_{d \in \mathcal{D}} l(w, x_d, y_d)$ to be minimized, where $\mathcal{D}$ is the combined dataset available $\mathcal{D} = \bigcup_{k=1}^{N} D_k$, and $l(w, x_d, y_d)$ represents the particular error between $y_d$ and the model output on $x_d$ (e.g., the squared distance). Thus, we aim to find $w$ that minimizes $f(w)$ over the data $\mathcal{D}$ in the network. In federated learning setting, this minimization is not performed directly, as each device $k$ only has access to $D_k$. We further define $F_k(w) = \frac{1}{|D_k|} \sum_{d \in D_k} l(w, x_d, y_d)$ as the local loss function at $k$ over $D_k$. If we assume that $|D_i| = |D_j| \forall i, j$, i.e., each device contains the same number of data points, we can simplify and express the optimization as an average over $F_k(w)$:

$$\min_w f(w) = \min_w \frac{1}{N} \sum_{k=1}^{N} F_k(w). \quad (1)$$

In general cases, devices may possess different amounts of data, e.g., due to data heterogeneity and varying compute capabilities. In such cases, we can replace the factor $1/N$ with $p_k = |D_k|/|\mathcal{D}|$ for a weighted average of the $F_k(w)$ [8], [12].

Federated learning algorithms differ in how (1) is solved. In our case, we will assume that a central server is available to orchestrate the learning across the devices. Such a scenario is increasingly common in fog or edge computing systems, where an edge server may be connected to edge devices, e.g., in a smart factory [12]. We will next introduce the standard algorithms for federated learning in these environments.

B. Inherent heterogeneity in edge learning systems

We consider the presence of various heterogeneity sources commonly manifested in practical edge computing systems:

1. **Data heterogeneity**: The generating distributions of data in devices are different. Data in a particular device depend on the distinct factors, e.g., usage, geographic location. Prior works usually need to assume some form of bounded dissimilarity across devices.

2. **Computational heterogeneity**: The computing resources at different devices vary that leads to the fact that some
devices can perform local optimization to near optimality while others only change the parameters slightly or may not optimize at all.

3. Communication heterogeneity: The latency between devices and the aggregation server is also non-homogeneous.

C. Federated learning algorithms and context definition

Algorithm 1: FedAvg - Federated learning with simple averaging.

Input : $K, T, w^{0}, N$

\begin{algorithmic}[1]
\FOR {$t = 0, \ldots, T - 1$}
\STATE Server samples a small set $S_t$ of $K$ devices uniformly at random.
\STATE Server sends $w^t$ to all devices $k \in S_t$.
\STATE Each device $k \in S_t$ finds a $w^{t+1}_k$ that optimizes the local loss function at device $k$.
\STATE Each device $k \in S_t$ sends $w^{t+1}_k$ back to the server.
\STATE Server aggregates the $w^{t+1}_k$, $\forall k \in S_t$ according to (2) to form a $w^{t+1}$.
\ENDFOR
\end{algorithmic}

The first federated learning algorithm, FedAvg [1], is summarized in Algorithm 1. Essentially, FedAvg selects random $K$ devices in each round to perform local optimization based on their individual data, and then averages all updated model parameters from those devices:

\begin{equation}
    w^{t+1} = \frac{1}{K} \sum_{k \in S_t} w^{t+1}_k.
\end{equation}

FedProx [8] is a recent improvement of FedAvg and differs from FedAvg by adding a proximal term, i.e., $\mu \| w - w^t \|^2_2$ at round $t$ with proximal parameter $\mu$, to the local objective function, $F_k(w)$, to regulate the changes made at the local device. Specifically, this proximal term will prevent the updated parameters from deviating too much from the global ones and, hence, from those of other devices as well. FedProx was shown in [8] to have linear convergence rate under assumptions on the near-convex loss functions, dissimilarity between local datasets. In practice, FedProx also performs better than FedAvg in terms of accuracy, however, the performance is still unstable. Similar idea has also been investigated in a recent work [9].

FOLB [11] studies the aggregation algorithm at the central server and proposes a smart weighted averaging that takes into account the inner products between local and global gradients with respect to the current model parameters. The underlying motivation is that devices with local gradients similar to the global one give updates in the right directions. On the other hand, for devices with dissimilar local gradients, we should consider the opposite update directions.

We define the context of an optimization round as follows:

**Definition 1** (Context). The context of an optimization round $t$ is defined to be the set $\{w^{t+1}_k, \forall k \in S_t\}$.

The context captures well the heterogeneity of participating devices in a specific round. Devices with more challenging data (incur large loss by the current model) or those with more computational resources will make major updates, thus, we should consider these more important than the others. FedAvg and FedProx employ simple averaging, leading to both slow convergence and unstable performance, while FOLB considers context with multiple assumptions on near convexity, data dissimilarity, and smoothness, limiting its effectiveness in the majority of practical applications.

III. Contextual Model Aggregation

We consider the same selection of a small set of $K$ devices uniformly at random similarly to FedAvg and FedProx, however, instead of simply averaging updated parameters from local devices, we propose a contextual aggregation scheme that results in an optimal context-dependent bound. In the following, we give details of the assumption made (Subsection III-A), derive context-dependent bound and its optimization (Subsection III-B), and then extend to the expected bound over random device selection (Subsection III-C).

A. Assumptions

Our proposed method is general, i.e., work for both convex and non-convex loss functions, and make the minimal smoothness assumption that the overall loss function $f(w)$ is $\beta$-smooth with respect to $w$. Note that this smoothness assumption is prevalent and essential in the literature of both convex and non-convex optimizations. The following property of smooth functions is extensively used in this work:

**Property 1** (Smoothness). Given a $\beta$-smooth function $f(x)$ with respect to $x$ and $x_1, x_2$ in the domain of $f(.)$, we have the following inequality,

\begin{equation}
    f(x_2) \leq f(x_1) + \langle \nabla f(x_1), x_2 - x_1 \rangle + \frac{\beta}{2} \| x_2 - x_1 \|^2_2. \tag{3}
\end{equation}

B. Deriving an aggregation scheme with optimal context-dependent bound

We will start from a general form of model aggregation associated with a set of variables and the $\beta$-smoothness property of function $f(w)$ to obtain a general lower-bound of loss reduction from the context of selected devices $S_t$ in round $t$. Then, we optimize the resulting bound over the aggregation variables to find the optimal setting. We explore practical considerations of parameters involved in the process and show a definite reduction off the loss function after every round of optimization.

Given a set of devices $S_t$ at round $t$ with the corresponding updated parameters $w^{t+1}_k, \forall k \in S_t$, we first consider a general form of aggregation that adjusts each update $\Delta w^{t+1}_k = w^{t+1}_k - w^t$ from device $k$ by a weight parameter $\alpha^t_k$.

\begin{equation}
    w^{t+1} = w^t + \sum_{k \in S_t} \alpha^t_k \Delta w^{t+1}_k. \tag{4}
\end{equation}

The weight parameter $\alpha^t_k$ reflects the importance of update from device $k$ in reducing the overall loss function $f(.)$ and must
optimally factors in all of the different sources of heterogeneity from data distribution to device’s available resources, which translates into how much the device optimizes the parameters based on its local data. From there, we use the property of $\beta$-smoothness of the function $f(w)$ to derive the following lower-bound on the loss reduction after round $t$:

$$f(w^{t+1}) \leq f(w^t) + \langle \nabla f(w^t), w^{t+1} - w^t \rangle + \beta \frac{1}{2} \| w^{t+1} - w^t \|_2^2 \leq f(w^t) + \langle \nabla f(w^t), \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \rangle + \beta \frac{1}{2} \| \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \|_2^2. \quad (5)$$

Thus,

$$f(w^t) - f(w^{t+1}) \geq - \left( \langle \nabla f(w^t), \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \rangle \right) + \frac{\beta}{2} \| \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \|_2^2. \quad (6)$$

The left hand side of (6) depicts the reduction of $f(w)$ after aggregation and the right hand side provides a lower-bound on that reduction. We would want to maximize this lower-bound or, equivalently, minimize the following function

$$g_t(\alpha^t) = \langle \nabla f(w^t), \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \rangle + \frac{\beta}{2} \| \sum_{k \in S_t} \alpha_k \Delta w_{k}^{t+1} \|_2^2,$$

where $\alpha^t = [\alpha_1^t, \ldots, \alpha_{n^t}^t]$. This bounding function depends on the updates $\Delta w_{k}^{t+1}$ from the current set of devices $S_t$ and weights $\alpha_k^t$. Thus, we call it context-dependent and refer to this as the lower-bound function of $\alpha_t$. We will find $\alpha_t$ to make this function as small (negative) as possible.

To derive the optimal $\alpha_t^*$ that minimizes the lower-bound function, we first look at the partial derivatives of $g_t(\alpha^t)$ with respect to $\alpha_k^t$ as follows:

$$\frac{\partial g_t(\alpha^t)}{\partial \alpha_k^t} = \langle \nabla f(w^t), \Delta w_{k}^{t+1} \rangle + \beta \sum_{k' \in S_t} \alpha_{k'}^t \langle \Delta w_{k}^{t+1}, \Delta w_{k'}^{t+1} \rangle = \langle \Delta w_{k}^{t+1}, \nabla f(w^t) \rangle + \beta \sum_{k' \in S_t} \alpha_{k'}^t \Delta w_{k'}^{t+1}. \quad (7)$$

The optimal solution satisfies $\frac{\partial g_t(\alpha^t)}{\partial \alpha_k^t} = 0, \forall k \in S_t$. Thus, $\nabla f(w^t) + \beta \sum_{k' \in S_t} \alpha_{k'}^t \Delta w_{k'}^{t+1}$ lives in the nullspace of a matrix $G_t$ that has $K$ rows corresponding to $\Delta w_{k}^{t+1}, \forall k \in S_t$. With presence of various heterogeneity sources, this matrix $G_t$ likely has full rank and, hence, its nullspace has rank of $n - K$, where $n$ is the dimension of model parameters $w$, based on the Rank Plus Nullity Theorem [13] with $K \ll n$. Hence, we need to find $\alpha_{k'}^t, k' \in S_t$ such that $\nabla f(w^t) + \beta \sum_{k' \in S_t} \alpha_{k'}^t \Delta w_{k'}^{t+1}$ lives in the nullspace of $G_t$. To achieve that, we first obtain a basis of the nullspace of $G_t$ through standard techniques in linear algebra [14], e.g., SVD. Let the basis consist of vectors $e_1, \ldots, e_{n-K}$ in $n$ dimension. Since every element in this nullspace is of the form $\sum_{i=1}^{n-K} x_i e_i$, we will solve the following equation:

$$\nabla f(w^t) + \beta \sum_{k' \in S_t} \alpha_{k'}^t \Delta w_{k'}^{t+1} = \sum_{i=1}^{n-K} x_i e_i, \quad (8)$$

for $\alpha_{k'}^t, k' \in S_t$ and $x_i, i = 1, \ldots, (n - K)$. Note that (8) is a system of $n$ linear equations and $n$ variables and can be solved quickly. The resulting $\alpha_{k'}^t, k' \in S_t$ will be used in our aggregation scheme to obtain a tight (optimal) lower-bound and leads to a better convergence rate.

**Proposition 1 (Optimality).** The aggregation in (4) with $\alpha_{k'}^t, k' \in S_t$ being the solution of the system of linear equations in (8) produces the optimal context-dependent bound in (5).

**Setting up parameters:** In the equation (8), we only have $\Delta w_{k'}^{t+1}$ available and need to determine the settings of smoothness constant $\beta$ and global gradient $\nabla f(w^{t^i})$. Since $\beta$ is generally unknown in advance, however, in smooth function optimizations [15], the ideal learning rate $l$ is set to $\frac{1}{\beta}$ for fast convergence rate. Thus, we set $\beta = \frac{1}{l}$ in the above equation (8), where $l$ is the learning rate of the local optimizers at devices. Moreover, $\nabla f(w^{t^i})$ is also generally not available (requiring all the devices to compute), in practice, we select a second set of $K_2$ random devices at each round just to compute the local gradients with respect to $w^t$ and average those local gradients to obtain an estimate of $\nabla f(w^{t^i})$. Specifically, in our experiments, we consider and compare various settings of $K_2$ and find that even in the extreme case of $K_2 = 0$, we can just use devices in $S_t$ to obtain an estimate of $\nabla f(w^t)$ and achieve nearly the same performance as when we use all $N$ devices to compute $\nabla f(w^t)$. Note also that this estimation step can be done in parallel with the local updates and is much faster than the later as well.

**Note on efficiency:** For machine learning models with a large number of parameters, e.g., deep neural networks, finding nullspace of $Q_t$ and solving (8) may render some computational challenges at the central server. Fortunately, oftentimes, we can make use of special features of the individual model type to improve efficiency. For example, in deep neural networks, prior studies [16]–[18] show that, with standard techniques of weight initialization and activation normalization, variation of gradient/update is mostly captured by that of the last layer’s parameters. Hence, we can use a small fraction, corresponding to the last layer’s parameters, of the gradient $\Delta w_{k'}^{t+1}$ and updates $\Delta w_{k'}^{t+1}$ as good approximations of the full versions.

**Contextual aggregation scheme:** Our new aggregation scheme is described in Algorithm 2. The first step is to compute a basis of the nullspace of matrix $G_t$. Note that this is quick since $G_t$ has only a small number of rows, $K$. Then, we solve (8) to find $\alpha_t^*$ that minimizes the lower-bound function, which is used in Line 3 to aggregate $\Delta w_{k'}^{t+1}$ and form the new set of model parameters $w_{t+1}^{t+1}$.

With this aggregation scheme in Algorithm 2, we obtain the
Algorithm 2: Contextual aggregation scheme towards optimal convergence.

**Input:** \( \nabla f(w^t), \Delta w_{k+1}^t, k \in S_t \)

1. Compute a basis of the nullspace of \( G_t \) formed by stacking \( \Delta w_{k+1}^t, \forall k \in S_t \) for rows of this matrix.
2. Solve the system of linear equations in (8) to find \( \alpha_k^t, \forall k \in S_t \) and \( x_i, \forall i = 1..(n - k) \).
3. Use \( \alpha_k^t, \forall k \in S_t \) to compute the next global model parameter set \( w^{t+1} \) according to (4).

following results related to convergence rate of the associated federated learning algorithm.

**Theorem 1** (Definite loss reduction). With the assumption that the function \( f(w) \) is \( \beta \)-smooth, the federated learning algorithm with aggregation scheme in Algorithm 2 provides the following loss reduction at each optimization round:

\[
\frac{f(w^t) - f(w^{t+1})}{\beta} \geq \frac{\sum k \in S_t \alpha_k^t \Delta w_{k+1}^t}{2}. 
\]  

(9)

**Proof.** Recall that \( \alpha_k^t, \forall k \in S_t \) satisfy,

\[
\frac{\partial f(\alpha^t)}{\alpha_k} = \langle \Delta w_{k+1}^t, \nabla f(w^t) + \beta \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \rangle = 0.
\]  

(10)

Combining the above identity with the lower-bound in (5) gives us the following derivation,

\[
\begin{align*}
&f(w^{t+1}) \leq f(w^t) + \langle \nabla f(w^t), \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \rangle \\
&\quad + \frac{\beta}{2} \left\| \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2 \\
&= f(w^t) + \langle \nabla f(w^t), \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \rangle \\
&\quad + \beta \left( \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \sum k' \in S_t \alpha_k^t \Delta w_{k+1}^t \right) \\
&\quad - \frac{\beta}{2} \left\| \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2 \\
&= f(w^t) + \sum k \in S_t \alpha_k^t \langle \Delta w_{k+1}^t, \nabla f(w^t) + \beta \sum k' \in S_t \alpha_k^t \Delta w_{k+1}^t \rangle \\
&\quad = 0 \text{ (due to (10))} \\
&\quad - \frac{\beta}{2} \left\| \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2 \\
&= f(w^t) - \frac{\beta}{2} \left\| \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2. \\
\end{align*}
\]

(11)

That completes the proof.

**Remark:** Note that we make no further assumption other than the minimal \( \beta \)-smoothness of the loss function \( f(w) \).

In comparison, previous works commonly rely on convexity, bounded gradient, gradient and Hessian dissimilarity in order to bound loss reduction. Thus, our method is quite general and applicable in a much larger number of cases. Furthermore, the contextual aggregation can be used as a modular plug-and-run component in many existing federated learning algorithms by simply replacing the vanilla aggregation with the contextual one. This allows for great flexibility at the local devices to choose the most suitable optimizer with respect to availability and computing resources. In fact, we demonstrate the combinations of our contextual aggregation with different local optimizations and show significant improved convergence rates compared to that of the existing federated learning algorithms.

The loss reduction in Theorem 1 depends primarily on the updates \( \Delta w_{k+1}^t, \forall k \in S_t \), which are the results of local optimization. Hence, if we consider a particular local optimizer, we can bound the updates and further derive a more detailed bound. However, the calculation of \( \alpha_k^t \) depends on \( \Delta w_{k+1}^t, \forall k \in S_t \) in a non-trivial way and a clean version of this bound without \( \alpha_k^t \) is difficult to obtain. Moreover, with additional assumptions on gradient dissimilarity and SGD as the local optimizer, we can derive formal convergence rate.

**C. Deriving a scheme with optimal expected bound**

Here we derive an aggregation scheme to maximize the expected loss reduction in round \( t \) over the randomness of device selection. The context-dependent bound may vary between different selections of participants and we are interested in optimizing the expected bound over all different choices. From (5), we take the expectation with respect to the random selection of devices in round \( t \) and obtain,

\[
\begin{align*}
\mathbb{E}[f(w^{t+1})] &\leq f(w^t) + \mathbb{E} \left[ \left\| \nabla f(w^t), \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2 \right] \\
&\quad + \frac{\beta}{2} \mathbb{E} \left[ \left\| \sum k \in S_t \alpha_k^t \Delta w_{k+1}^t \right\|^2_2 \right] \\
&= f(w^t) + \frac{K}{N} \sum k = 1 \alpha_k^t \langle \nabla f(w^t), \Delta w_{k+1}^t \rangle \\
&\quad + \frac{\beta}{2} \mathbb{E} \left[ \left\| \sum k, k' \in S_t \alpha_k^t \alpha_{k'}^t \langle \Delta w_{k+1}^t, \Delta w_{k'-1}^t \rangle \right\|^2_2 \right]. \\
\end{align*}
\]  

(12)

then,

\[
\begin{align*}
\mathbb{E}[f(w^t) - f(w^{t+1})] &\geq - \left( \frac{K}{N} \sum k = 1 \alpha_k^t \langle \nabla f(w^t), \Delta w_{k+1}^t \rangle \\
&\quad + \frac{\beta}{2} \mathbb{E} \left[ \left\| \sum k, k' \in S_t \alpha_k^t \alpha_{k'}^t \langle \Delta w_{k+1}^t, \Delta w_{k'-1}^t \rangle \right\|^2_2 \right] \right). \\
\end{align*}
\]  

(13)

Similarly to the case of context-dependent bound, let \( g_i(\alpha^t) \) be the lower-bound function - negated right-hand side of the
above inequality, and taking derivatives of $g_t(\alpha^t)$ with respect to $\alpha^t_k$ gives us:

$$\frac{\partial g(\alpha^t)}{\partial \alpha^t_k} = \frac{K}{N} \langle \nabla f(w^t), \Delta w^{t+1}_k \rangle + \beta \frac{K(K-1)}{N(N-1)} \sum_{k'=1}^{N} \alpha^t_{k'} (\Delta w^{t+1}_k, \Delta w^{t+1}_{k'}) = \langle \Delta w^{t+1}_k, \frac{K}{N} \nabla f(w^t) \rangle + \beta \frac{K(K-1)}{N(N-1)} \sum_{k'=1}^{N} \alpha^t_{k'} \Delta w^{t+1}_{k'} \rangle.$$

We need to solve $\frac{\partial g(\alpha^t)}{\partial \alpha^t_k} = 0, \forall k \in 1..N$, and can follow the same footsteps as with the context-dependent bound. However, we would need $\Delta w^{t+1}_k, \forall k = 1..N$, or, in other words, the full participation of all the devices in the entire network. There are many prior research works [19], [20] (see surveys [2], [3], [21]) that consider the full participation setting and we can apply our techniques to find an optimal $\alpha^t$ in those cases. On the other hand, if this setting of full participation is not feasible, e.g., in the original federated learning framework [1], an approximation can be obtained by sampling a much smaller pool of $N'$ devices in each round of optimization and solve for $\alpha^t$ that is composed of $\alpha''_k, \forall k \in S_t$ and $N'$ auxiliary variables $x_i$. The resulting $\alpha''_k, \forall k \in S_t$ will then be used in the aggregation scheme. In addition, the settings of $\beta = \frac{1}{2}$ and an estimate of $\nabla f(w^t)$ can be obtained in a similar manner as in the context-dependent bound.

Clearly, the resulting bound will not be a definite reduction of loss, but rather, a positive bound on improvement of expected loss. Furthermore, compared to the case of context-dependent bound, solving for $\alpha^t_k$ would require more computation since the matrix $Q_t$ has $N$ rows, instead of $K$, and finding a basis of $Q_t$ nullspace is more expensive.

IV. EXPERIMENTS

In this section, we present our experimental results to demonstrate the advantages of our contextual aggregation scheme when combined with different existing federated learning algorithms. We show that these combinations offer both faster convergence speed and more robust performance throughout the entire optimization process compared with existing state-of-the-art approaches.

A. Experimental setup

1) Datasets with data heterogeneity: We adopt four datasets commonly used in the literature [2], [11], [22]-[24]: 10-class MNIST [25], 62-class Federated Extended MNIST (FEMNIST) [26], and two synthetic datasets to simulate different levels of data heterogeneity [22], [23]. The two synthetic datasets, namely Synthetic IID and Synthetic_1_1, corresponds to scenarios with the i.i.d. data and a high level of data heterogeneity across devices in the network (see [22] for details). We also consider the commonly used multinomial logistic regression as the underlying machine learning model to perform classification tasks on the datasets.

2) Federated learning algorithms: To demonstrate the flexibility and effectiveness of the proposed contextual aggregation scheme, we combine it with standard federated learning algorithms by replacing the existing aggregation by the contextual one. In particular, we consider on the canonical FedAvg [1] and denote its contextual version by FedAvg (Contextual), and the recent state-of-the-art FedProx [8] with the contextual variant FedProx (Contextual). In addition, we also compare with the recent algorithm FOLB [11], which is equipped with a smart weighted averaging aggregation on top of FedProx. Thus, FOLB represents the state-of-the-art aggregation to compare with the proposed scheme. In all the algorithms, we fix the number of devices in each round to 10, $K = 10$, which is also standard in the literature.

In all the experiments, we consider the more efficient aggregation with context-dependent bound in Subsection III-B. Moreover, we also examine different variants of the contextual aggregation by varying $K_2$ - the number of devices for estimating $\nabla f(w^t)$. Explicitly, we vary $K_2$ between $N$ and 0, (i.e., $N, 50, 20, 10, 0$). For the case $K_2 = 0$, we just use the same devices in $S_t$ to estimate $\nabla f(w^t)$.

3) Local optimization and computational heterogeneity: We use mini-batch SGD as local optimizer and simulate devices’ heterogeneity of computing resources by allowing each device to perform a random number of epochs uniformly selected between 1 and 20. Moreover, all these random selections are kept consistent across all the algorithms and settings by initializing the random number generator for device selection with the same seed.

4) Metrics: To study the performance, we report the training loss and test accuracy of the trained model after a certain number of rounds. We also inspect the number of rounds each algorithm requires to achieve a certain level of test accuracy to compare the convergence speeds.

B. Experimental results

We first study different variants of our contextual aggregation scheme and then compare them with the existing FL algorithms in terms of performance and robustness.

1) Comparison between contextual variants: This first set of experiments focuses on variants of the proposed contextual aggregation scheme with varying $K_2$ - number of devices to estimate the global gradient $\nabla f(w^t)$ in each round $t$. We show that a very small number of devices is sufficient to achieve the top performance of the contextual aggregation. We use FedProx (Contextual) with various settings of the proximal parameter $\mu$ (see [8] for more details), since proximal local optimization has witnessed numerous successes in dealing with data heterogeneity in federated learning [8], [9]. These experiments are run on MNIST dataset.

Figures 2 and 3 display the training loss and test accuracy of the examined variants. The results reveal an interesting characteristic that even with a very small value of $K_2$, the performance is still near the peak at $K_2 = N$. Specifically, the variants $K_2 = N, K_2 = 50, K_2 = 20$, and $K_2 = 10$, have visually indistinguishable performance in both training
Fig. 2: Training loss comparison of different aggregation variants in various settings with FedProx (Contextual). All the variants of contextual aggregation deliver similar performance, even in the most extreme case with $K_2 = 0$.

Fig. 3: Test accuracy comparison of different aggregation variants in various settings.

Fig. 4: Training loss comparison of different federated learning algorithms in various settings. The contextual versions significantly outperform the existing algorithms in both achieving better performance metrics and robustness between rounds of optimization.

Fig. 5: Test accuracy comparison of different federated learning algorithms in various settings.

loss and test accuracy. We only observe some differences in the extreme case of $K_2 = 0$, where we need to use the same set of devices $S_t$ to both estimate $\nabla f(w^t)$ and perform local updates. However, the differences are negligible and appear as minor fluctuations from the ideal case of $K_2 = N$. The reason for these differences is likely due to correlation between the estimated $\nabla f(w^t)$ and the updated parameters from the same set of devices. This correlation is broken when $K_2 > 0$ and our aggregation performs near optimality as illustrated by the results of other variants.

Another observation is the fast convergence and robust performance of all the variants. They all converge after about 20 rounds of optimization and remain at the same peak level of minimum loss and maximum accuracy. There is also not much difference between the results with distinct values of proximal parameter $\mu$ indicating that any advantage in performance will be attributed to the core contextual aggregation and not to the proximal terms added to local optimization. Henceforth, we would expect FedAvg (Contextual) and FedProx (Contextual) to perform similarly in subsequent experiments.

2) Optimal aggregation variables: In Figure 7, we plots the computed aggregation variables $\alpha_k^t$, $k \in S_t$ at different rounds...
Fig. 6: Number of optimization rounds to reach different accuracy levels required by federated learning algorithms on various datasets ($\mu = 0.1$ for FedProx and variants). The contextual versions require much fewer rounds to achieve the same levels of accuracy compared with the original algorithms.

Fig. 7: Vastly different aggregation variables computed at the early, near-converged and converged stages.

---

3) Comparison between contextual federated learning and existing algorithms: We compare the contextual versions, FedAvg (Contextual) and FedProx (Contextual), with the original FedAvg and FedProx, and the recent FOLB with a smart aggregation scheme.

Figures 4 and 5 illustrate training loss and test accuracy of all the considered algorithms on MNIST dataset. In both metrics, the contextual versions noticeably converge faster and are robust throughout the optimization rounds than both FedAvg, FedProx, and FOLB in all the experiments. The curves produced by contextual aggregation are always better (lower in loss and higher in accuracy) than the rest and very smooth. As also shown in numerous studies [2], [8], [11], FedAvg and FedProx show great fluctuations in performance even between consecutive rounds due to data heterogeneity. FOLB achieves better results than FedAvg and FedProx in individual rounds, however, it suffers from the same fluctuations, especially with smaller values of the proximal constant $\mu$. This shows the same role. This is in contrast with the common simple averaging in FedAvg, FedProx and most prior works.
the ineffectiveness of the aggregation algorithm of FOLB in dealing with the robustness issue in federated learning. In contrast, our contextual versions provide both higher results and great robustness in improving performance after each round or maintaining the same peak level after converged. The results here experimentally verify the property of our contextual aggregation that it definitely reduces the loss value for a broad class of functions.

As expected, FedAvg (Contextual) and FedProx (Contextual) perform markedly the same. This shows that contextual aggregation addresses well data heterogeneity and nullifies the effect of proximal term. On the other hand, FedProx with large $\mu$ shows some margins to FedAvg thanks to the proximal term in local optimization to mitigate data heterogeneity as shown in [8]. However, we also take into account the inherent computing resource heterogeneity across local devices, thus, both FedAvg and FedProx exhibit slow convergence and ample performance instability between rounds.

Figure 6 gives a broader view of the number of rounds required by the tested federated algorithms to attain various levels of accuracy, i.e., 50%, 60%, 70%, and 80%, on all the datasets to demonstrate the convergence speed. On the two real datasets, MNIST and FEMNIST, the contextual versions reduce the number of rounds required by the original algorithms by a factor of 3 or more consistently across all levels of accuracy. Compared to FOLB, our contextual algorithms also reduce the number of rounds by 2 times. On the i.i.d. dataset Synthetic_ID, FOLB, FedProx, and the two contextual algorithms perform similarly and are much better than FedAvg. This shows that in the i.i.d. case, most algorithms already achieve good performance. However, in the highly non-i.i.d. case of Synthetic_1_1, both FedAvg and FedProx fall short again due to the issues with data heterogeneity. FOLB and our contextual algorithms all require small number of rounds to reach the specified accuracy levels. Hence, both the weighted aggregation in FOLB and our contextual scheme work well in this synthetic dataset with a high level of heterogeneity.

V. RELATED WORKS

Federated learning falls under the umbrella of distributed optimization, which has been studied extensively in the literature [27], [28]. However, early works on distributed optimization focused on datacenter or cloud-based scenarios where shareable data are distributed across a relatively small number of nearby powerful machines, and communication cost as well as privacy are not an issue in traditional setup. However, federated learning targets the massive networks of mobile devices with much slower communication and data privacy is a primary concern. A vast amount of work [1], [2], [4], [7]–[10], [19], [29], [30] has studied the new challenges and optimization algorithms in this setting.

FedAvg [1] is the first and likely most popular federated learning algorithm due to its simplicity and effectiveness. Different from earlier works in distributed optimization, FedAvg employs multiple epochs of local SGD as optimizer in each round. The updated parameters from a small random set of devices are averaged to serve as the new global model. Later works in [7], [8], [10], [23], [31] analyzed convergence rate of FedAvg under assumptions on convexity, bounded gradient, and bounded dissimilarity between devices. Other works [8], [9] improved over FedAvg by introducing a proximal term into local loss functions to mitigate data heterogeneity and make the loss strongly convex. With similar goal, the work in [10] introduces a control variate to local updates as a correction mechanism to combat data heterogeneity. The issue with control variate is that all the devices are stateful that means each device needs to maintain a control variate the entire time and may not even be used due to random selection of devices to participate. In contrast to these works, we allow any local optimizer to be used under the effect of devices’ heterogeneity, and focus our attention on the more resourceful central server, that performs aggregation of local updates. With more computing capability, the server should be able to evaluate the usefulness of each update and combine them in an optimal way that maximally reduces the overall loss function.

Most related to our work is the recent FOLB algorithm in [11]. FOLB builds on top of FedProx [23] and subsumes a smart aggregation scheme that weighs each local update by the inner product between the local and global gradients. This inner product effectively determines whether the update performed at the device are on the right direction with respect to the global gradient. In cases where 1) the loss function is smooth, 2) local losses are near convex, and 3) gradient dissimilarity between devices is founded, FOLB can reduce the expected loss and improve over FedProx. Different from FOLB, the proposed contextual aggregation scheme only uses the smoothness assumption of the overall loss function while providing definite loss reduction in every round of optimization. Our experimental results in Section IV show significantly better convergence speed and robustness of our contextual aggregation scheme over that in FOLB.

Other related works include [19], [20], [32] that consider full participation of all devices in every round and also study offloading data to improve convergence speed. [33]–[36] which studies federated learning over wireless networks. Comprehensive surveys can be found in [2], [4].

VI. CONCLUSION

We have proposed contextual aggregation algorithms in federated learning that obtains an optimal bound on loss reduction and demonstrated both faster convergence speed and high level of robustness during the optimization process. The proposed aggregations can be integrated into many existing algorithms and provide significant improvements over the vanilla versions. We have considered multiple variants of the proposed approach and compared them with state-of-the-art federated learning algorithms to illustrate the advantages of our solutions.

Our future works include implementing the contextual federated learning algorithms in practical edge computing systems and investigating performance under this setting as well as possible issues arisen in practical systems.
REFERENCES

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proceedings of the Artificial Intelligence and Statistics. PMLR, 2017, pp. 1273–1282.

[2] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, “Federated learning: Challenges, methods, and future directions,” 2019, arXiv preprint arXiv:1908.07873.

[3] Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, and H. Yu, “Federated learning,” Synthesis Lectures on Artificial Intelligence and Machine Learning, vol. 13, no. 3, pp. 1–207, 2019.

[4] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings et al., “Advances and open problems in federated learning,” 2019, arXiv preprint arXiv:1912.04977.

[5] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, “On the convergence of fedavg on non-iid data,” 2019, arXiv preprint arXiv:1907.02189.

[6] H. Yu, S. Yang, and S. Zhu, “Parallel restarted sgd with faster convergence and less communication: Demystifying why model averaging works for deep learning,” in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, no. 01, 2019, pp. 5693–5700.

[7] A. Khaled, K. Mishchenko, and P. Richtárik, “Tighter theory for local sgd on identical and heterogeneous data,” in Proceedings of the International Conference on Artificial Intelligence and Statistics. PMLR, 2020, pp. 4519–4529.

[8] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” 2020, arXiv preprint arXiv:1812.06127.

[9] C. T. Dinh, N. H. Tran, and T. D. Nguyen, “Personalized federated learning with moreau envelopes,” 2020, arXiv preprint arXiv:2006.08848.

[10] S. P. Karimireddy, S. Kale, M. Mohri, S. Reddi, S. Stich, and A. T. Suresh, “Scaffold: Stochastic controlled averaging for federated learning,” in Proceedings of the International Conference on Machine Learning, PMLR, 2020, pp. 5132–5143.

[11] H. Yu, R. Jin, and S. Yang, “On the linear speedup analysis of communication efficient momentum sgd for distributed non-convex optimization,” 2019, arXiv preprint arXiv:1905.03817.

[12] F. P.-C. Lin, S. Hosseinalipour, S. S. Azam, C. G. Brinton, and N. Michelusi, “Two timescale hybrid federated learning with cooperative d2d local model aggregations,” 2021, arXiv preprint arXiv:2103.10481.

[13] Y.-S. Jeon, M. M. , J. Li, and H. V. Poor, “Gradient estimation for federated learning over massive mimo communication systems,” 2020, arXiv preprint arXiv:2003.08059.

[14] M. M. Amiri, D. Gündüz, S. R. Kulkarni, and H. V. Poor, “Convergence of update aware device scheduling for federated learning at the wireless edge,” IEEE Transactions on Wireless Communications, vol. 20, no. 6, pp. 3643–3658, 2021.

[15] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, “A joint learning and communications framework for federated learning over wireless networks,” 2019, arXiv preprint arXiv:1909.07972.

[16] M. Chen, H. V. Poor, W. Saad, and S. Cui, “Convergence time optimization for federated learning over wireless networks,” 2020, arXiv preprint arXiv:2001.07845.

[17] X. Li, K. Huang, W. Yang, S. Wang, and Z. Zhang, “On the convergence of fedavg on non-iid data,” 2019, arXiv preprint arXiv:1907.02189.

[18] T. Li, M. Sanjabi, and V. Smith, “Fair resource allocation in federated learning,” 2019, arXiv preprint arXiv:1905.10497.

[19] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[20] G. Cohen, S. Afshar, J. Tappson, and A. Van Schaik, “Emnist: Extending mnist to handwritten letters,” in Proceedings of the 2017 International Joint Conference on Neural Networks. IEEE, 2017, pp. 2921–2926.

[21] S. Boyd, N. Parikh, and E. Chu, Distributed Optimization and Statistical Learning via the Alternating Direction Method of Multipliers. Now Publishers Inc, 2011.

[22] V. Smith, S. Forte, C. Ma, M. Takac, M. I. Jordan, and M. Jaggi, “Cocoa: A general framework for communication-efficient distributed optimization,” 2016, arXiv preprint arXiv:1611.02189.

[23] H. Yu, S. Yang, and S. Zhu, “Parallel restarted sgd for non-convex optimization with faster convergence and less communication,” 2018, arXiv preprint arXiv:1807.06629.

[24] P. Jiang and G. Agrawal, “A linear speedup analysis of distributed deep learning with sparse and quantized communication,” in Proceedings of the 32nd International Conference on Neural Information Processing Systems, 2018, pp. 2530–2541.

[25] H. Yu, R. Jin, and S. Yang, “On the linear speedup analysis of communication efficient momentum sgd for distributed non-convex optimization,” 2019, arXiv preprint arXiv:1905.03817.

[26] S. Boyd, N. Parikh, and E. Chu, Convex optimization. Cambridge university press, 2004.

[27] G. Cohen, S. Afshar, J. Tappson, and A. Van Schaik, “Emnist: Extending mnist to handwritten letters,” in Proceedings of the 2017 International Joint Conference on Neural Networks. IEEE, 2017, pp. 2921–2926.

[28] P. Jiang and G. Agrawal, “A linear speedup analysis of distributed deep learning with sparse and quantized communication,” in Proceedings of the 32nd International Conference on Neural Information Processing Systems, 2018, pp. 2530–2541.

[29] H. Yu, R. Jin, and S. Yang, “On the linear speedup analysis of communication efficient momentum sgd for distributed non-convex optimization,” 2019, arXiv preprint arXiv:1905.03817.

[30] F. P.-C. Lin, S. Hosseinalipour, S. S. Azam, C. G. Brinton, and N. Michelusi, “Two timescale hybrid federated learning with cooperative d2d local model aggregations,” 2021, arXiv preprint arXiv:2103.10481.

[31] Y.-S. Jeon, M. M. , J. Li, and H. V. Poor, “Gradient estimation for federated learning over massive mimo communication systems,” 2020, arXiv preprint arXiv:2003.08059.

[32] M. M. Amiri, D. Gündüz, S. R. Kulkarni, and H. V. Poor, “Convergence of update aware device scheduling for federated learning at the wireless edge,” IEEE Transactions on Wireless Communications, vol. 20, no. 6, pp. 3643–3658, 2021.

[33] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, “A joint learning and communications framework for federated learning over wireless networks,” 2019, arXiv preprint arXiv:1909.07972.

[34] M. Chen, H. V. Poor, W. Saad, and S. Cui, “Convergence time optimization for federated learning over wireless networks,” 2020, arXiv preprint arXiv:2001.07845.