

Personalized Federated Learning for Heterogeneous Clients with Clustered Knowledge Transfer

Yae Jee Cho
 ECE Department
 Carnegie Mellon University
 Pittsburgh, PA 15213
 yaejee@andrew.cmu.edu

Jianyu Wang
 ECE Department
 Carnegie Mellon University
 Pittsburgh, PA 15213
 jianyuw1@andrew.cmu.edu

Tarun Chiruvolu
 School of Computer Science
 Carnegie Mellon University
 Pittsburgh, PA 15213
 tchiruvo@andrew.cmu.edu

Gauri Joshi
 ECE Department
 Carnegie Mellon University
 Pittsburgh, PA 15213
 gaurij@andrew.cmu.edu

Abstract

Personalized federated learning (FL) aims to train model(s) that can perform well for individual clients that are highly data and system heterogeneous. Most work in personalized FL, however, assumes using the same model architecture at all clients and increases the communication cost by sending/receiving models. This may not be feasible for realistic scenarios of FL. In practice, clients have highly heterogeneous system-capabilities and limited communication resources. In our work, we propose a personalized FL framework, PERFED-CKT, where clients can use heterogeneous model architectures and do not directly communicate their model parameters. PERFED-CKT uses *clustered co-distillation*, where clients use logits to transfer their knowledge to other clients that have similar data-distributions. We theoretically show the convergence and generalization properties of PERFED-CKT and empirically show that PERFED-CKT achieves high test accuracy with several orders of magnitude lower communication cost compared to the state-of-the-art personalized FL schemes.

1 Introduction

The emerging paradigm of federated learning (FL) [1–4] enabled the use of data collected by thousands of resource-constrained clients to train machine learning models without having to transfer the data to the cloud. Most recent work [5–8] is focused on algorithms for training a single global model with edge-clients via FL. However, due to the inherently high data-heterogeneity across clients [9–19], a single model that is trained to perform best in expectation for the sum of all participating clients’ loss functions may not work well for each client [20–22]. For example, if a single global model was trained for next-word prediction with all available clients and the input was “I was born in”, the model will most likely give bad results for the individual clients.

The limited generalization properties of conventionally trained FL models to clients with scarce local data calls for the design of FL algorithms to train personalized models that can perform well for individual clients. Several works have investigated personalized FL [23–26], including applying meta-learning [23], training separate models on each client with weighted aggregation of other clients’ models [24], using the global objective as a regularizer for training individual models at each client [25], or using model/data-interpolation with clustering for personalization [26]. However, the aforementioned work does not consider two critical factors of FL: i) the computation and memory capabilities can be heterogeneous across clients and ii) the cost of communicating high-dimensional models with the server can be prohibitively high [27, 28]. Most work in personalized FL assumes a homogeneous model architecture across clients, and frequent communication of the model parameters.

In this work, we propose training personalized models with clustered co-distillation. Co-distillation [29–31] is an approach to perform distributed training across different clients with reduced communication cost by only exchanging models’ predictions on a common unlabeled dataset instead of the model parameters. This method adds a regularization term to the local loss of each client to penalize the client’s prediction from being significantly different from the predictions of other clients. In the conventional co-distillation, the regularizing term for each client is the average of all other participating clients’ predictions. However in FL, clients’ data can be highly heterogeneous. Thus, forcing each client to follow the average prediction of all clients can exacerbate its generalization by learning irrelevant knowledge from clients that have significantly different data distributions [32]. Hence, we propose a novel *clustered co-distillation* framework **PERFED-CKT**, where each client uses the average prediction of only the clients that have similar data distributions. This way, we prevent each client from assimilating irrelevant knowledge from unrelated clients.

In short, **PERFED-CKT** largely improves on current personalized FL strategies in the following ways:

- Allows model heterogeneity across clients where the architecture and size of the model for local training can vary across clients.
- Dramatically reduces the communication cost by transferring logits instead of model parameters between the clients and the server.
- Improves generalization performance for data-scarce clients, while preventing learning from unrelated clients by clustered knowledge transfer.

We also present theoretical analysis of **PERFED-CKT** with its convergence guarantees and generalization performance. The generalization results show that clustering indeed helps in terms of improvement of the generalization properties of individual clients. Our experiments demonstrate that for both model-homogeneous and model-heterogeneous environments, **PERFED-CKT** can achieve high test accuracy with several orders of magnitude less communication.

2 Background and Related Work

Personalized FL. In personalized FL, the goal is to train a single or several model(s) that can generalize well to each client’s test dataset. In [23], using meta-learning for training a global model that better represents each client’s data was proposed. A similar line of work using the moreau envelope as a regularizer was proposed in [33]. Work in [24] proposed to find the optimal weighted combination of models from clients so that each client gets a model that better represents its target data distribution. The authors in [26] propose general approaches that can be applied to vanilla FL for personalization, including client clustering and data/model interpolation.

The aforementioned work however, all requires model homogeneity and direct communication of model parameters across clients/server. Although [34] does consider communication cost in personalization by using distillation, it does not provide any theoretical guarantees and does not consider the high data heterogeneity across clients that can tamper with the personalization performance. Moreover they require the presence of a *large labeled* public dataset, which is realistically an expensive resource to have access to. Our work investigates a novel personalized FL framework that allows model heterogeneity, improves communication-efficiency, and utilizes data heterogeneity with clustering while using a *small unlabeled* public dataset.

Knowledge Transfer. Knowledge distillation (KD) [35] is prominently used as a method of knowledge transfer from a pre-trained larger model to a smaller model [36–44]. Extending from this conventional KD, co-distillation [32, 45, 46] transfers knowledge across multiple models that are being trained concurrently. Specifically, each model is trained with the supervised loss with an additional regularizer term that encourages the model to yield similar outputs to the outputs of the other models that are also being trained.

Using co-distillation for improved generalization in distributed training has been recently proposed in [29–31]. Authors of [29] have shown empirically that co-distillation indeed improves generalization for distributed learning but often results in over-regularization, where the trained model’s performance drops due to overfitting to the regularization term. In [30], co-distillation was suggested for communication-efficient distributed training, but not in the personalized FL context where data

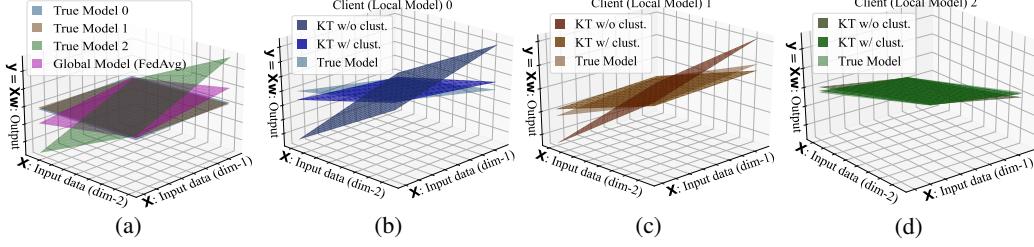


Figure 1: Toy example with linear regression for given input data $\mathbf{X} \in \mathbb{R}^2$ and local (true) models $\mathbf{w} \in \mathbb{R}^{2 \times 1}$ for three clients indexed by 0-2; (a): the true model for each client and the global model from FedAvg. The resulting global model does not match well with clients’ true model; (b)-(d): the model for each client resulting from PERFED-CKT with and without clustering (simple average of logits). PERFED-CKT with clustering yields the model closest to the true model for all clients.

can be highly heterogeneous across nodes and presented limited experiments on a handful of nodes with homogeneous data distributions across the nodes.

Applying co-distillation for personalized FL presents a unique challenge in that each client’s data distribution can be significantly different from other clients’ distributions. Using standard co-distillation with the entire clients’ models can actually worsen clients’ test performance due to learning irrelevant information from other clients with different data distributions. We show in our work that this is indeed the case and show that using clustering to find the clients that have similar data-distributions with each other and then performing co-distillation within the clusters improves the personalized model’s performance significantly for each client.

3 Proposed Personalized FL Framework: PERFED-CKT

Problem Formulation

Consider a cross-device FL setup where a large number of K clients (edge-devices) are connected to a central server. We consider a N -class classification task where each client $k \in [K]$ has its local training dataset \mathcal{B}_k with $|\mathcal{B}_k| = m_k$ data samples. We denote $p_k = m_k / \sum_{k=1}^K m_k$ as the fraction of data for client k . Each data sample ξ is a pair (\mathbf{x}, y) where $\mathbf{x} \in \mathbb{R}^d$ is the input and $y \in [1, N]$ is the label. The dataset \mathcal{B}_k is drawn from the local data distribution \mathcal{D}_k , where we denote the empirical data distribution of \mathcal{B}_k as $\widehat{\mathcal{D}}_k$. In the standard FL [1], clients aim to collaboratively find the model parameter vector $\mathbf{w} \in \mathbb{R}^n$ that maps the input \mathbf{x} to label y , such that \mathbf{w} minimizes the empirical risk $F(\mathbf{w}) = \sum_{k=1}^K p_k F_k(\mathbf{w})$. The function $F_k(\mathbf{w})$ is the local objective of client k , defined as $F_k(\mathbf{w}) = \frac{1}{|\mathcal{B}_k|} \sum_{\xi \in \mathcal{B}_k} f(\mathbf{w}, \xi)$ with $f(\mathbf{w}, \xi)$ being the composite loss function.

Due to high data heterogeneity across clients, the optimal model parameters \mathbf{w}^* that minimize $F(\mathbf{w})$ can generalize badly to clients whose local objective $F_k(\mathbf{w})$ significantly differs from $F(\mathbf{w})$. Such clients may opt out of FL, and instead train their own models $\mathbf{w}_k \in \mathbb{R}^{n_k}$ by minimizing their local objectives, where \mathbf{w}_k can be heterogeneous in dimension. This can work well for clients with a large number of training samples (i.e., large m_k), since their empirical data distribution $\widehat{\mathcal{D}}_k$ becomes similar to \mathcal{D}_k , ensuring good generalization. However, if clients have a small number of training samples, which is often the case [47], the distributions \mathcal{D}_k and $\widehat{\mathcal{D}}_k$ can differ significantly, and therefore a model \mathbf{w}_k trained only using the local dataset \mathcal{B}_k can generalize badly. Hence, although clients with small number of training samples are motivated to participate in FL, the clients may actually not benefit from FL due to the bad generalization properties coming from other clients with significantly different data distributions. We show that with our proposed PERFED-CKT, clients with small training samples still benefit from participating in FL, improving generalization by being clustered with clients with similar data distributions.

Objective with Clustered Knowledge Transfer. We use co-distillation across different clients in FL for personalization, where each client co-distills with only the other clients that have similar model outputs with its own model, namely, *clustered knowledge transfer*. With clustered knowledge transfer, each client learns from clients that have similar data distributions to improve its generalization

performance. Formally, we consider each client having access to its private dataset \mathcal{B}_k and a public dataset \mathcal{P} , consisting of *unlabeled* data. The public dataset \mathcal{P} is used as a reference dataset for co-distillation across clients¹. The classification models \mathbf{w}_k , $k \in [K]$ output soft-decisions (logits) over the pre-defined number of classes N , which is a probability vector over the N classes. We refer to the soft-decision of model \mathbf{w}_k over any input data \mathbf{x} in either the private or public dataset as $s(\mathbf{w}_k, \mathbf{x}) : \mathbb{R}^{n_k} \times (\mathcal{B}_k \cup \mathcal{P}) \rightarrow \Delta_N$, where Δ_N stands for the probability simplex over N . For notational simplicity, we define $\mathbf{s}_k \in \mathbb{R}^{|\mathcal{P}| \times N}$ as $s(\mathbf{w}_k, \mathbf{x}) \in \mathbb{R}^{1 \times N}$, $\mathbf{x} \in \mathcal{P}$ stacked into rows for each \mathbf{x} . We similarly define $\bar{\mathbf{s}}_k = \sum_{i=1}^K \alpha_{k,i} \mathbf{s}_i$.

The clients are connected via a central aggregating server. Each client seeks to find the model parameter \mathbf{w}_k that minimizes the empirical risk $\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k)$, where $\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k)$ is a sum of the empirical risk of its own local training data $F_k(\mathbf{w}_k)$ and the regularization term as follows:

$$\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k) = F_k(\mathbf{w}_k) + \underbrace{\frac{\lambda}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \|\bar{\mathbf{s}}_k(\mathbf{x}) - s(\mathbf{w}_k, \mathbf{x})\|_2^2}_{\text{regularization term}} \quad (1)$$

The term $\bar{\mathbf{s}}_k(\mathbf{x}) = \sum_{i=1}^K \alpha_{k,i} s(\mathbf{w}_i, \mathbf{x})$ denotes the weighted average of the logits from all clients for an arbitrary set of weights for client k , i.e., $\{\alpha_{k,i}\}_{i \in [K]}$ such that $\sum_{i=1}^K \alpha_{k,i} = 1$, $\forall k \in [K]$. The term λ modulates the weight of the regularization term. The weight $\alpha_{k,i}$ for each client i , $i \in [K]$ with respect to client k results from clustering the logits by the ℓ_2 -norm distance so that clients with similar logits will have higher weights for each others' logits. The aggregated logit information with weights, $\bar{\mathbf{s}}_k$, is calculated and sent by the server to the clients. Details of how the weights $\alpha_{k,i}$, $i \in [K]$ for each client k are calculated and how the logits are communicated are elaborated in more detail in the subsequent Algorithm subsection. Before going into details of the algorithm we first give more intuition on the formulation of the regularization term in the next paragraph.

Regularization Term. Without the regularization term in (1), minimizing $\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k)$ with regards to \mathbf{w}_k is analogous to locally training in isolation for minimizing the local objective function $F_k(\mathbf{w}_k)$ for client k . If we have the regularization term with $\alpha_{k,i} = 1/K$, $\forall k, i \in [K]$, co-distillation is implemented without clustering, using all of the clients' knowledge. We show in the next toy example and in a generalization bound derived for ensemble models in personalization in Appendix D of why setting the values $\alpha_{k,i}$, $k, i \in [K]$ via clustering is critical to improve personalization.

We consider a toy example with linear regression where we have three clients with true models as in Figure 1(a) where true model 0 and 1 are similar to each other but true model 2 is different. The global model trained from vanilla FedAvg does not match well with any true models as shown in Figure 1(a). If we minimize (1) with respect to \mathbf{w}_k without clustering, i.e., $\alpha_{k,i} = 1/K$, $\forall k, i \in [K]$, the output local model also diverges from the true model for each client, especially for client 0 and 1, due to the heterogeneity across the true models (see Figure 1(b)-(d)). Finally, if we minimize (1) with clustering so that for client k , higher weight $\alpha_{k,i}$ is given to the client i that has a similar true model to client k , and smaller weight is given to the other client that has a different true model, the output local model of client k gets close to its true model. This is further explored theoretically in Theorem 4.2. PERFED-CKT is based on this motivation where we set the weights for co-distillation in $\bar{\mathbf{s}}_k(\mathbf{x}) = \sum_{i=1}^K \alpha_{k,i} s(\mathbf{w}_i, \mathbf{x})$ so that each client k sets higher $\alpha_{k,i}$, $i \in [K]$ for client i that has smaller difference between $s(\mathbf{w}_i, \mathbf{x})$ and $s(\mathbf{w}_k, \mathbf{x})$. Details of the setup for Figure 1 are in Appendix E.

Algorithm.

We minimize (1) with respect to \mathbf{w}_k for each client k on its own device with only communicating the logits instead of the actual model \mathbf{w}_k , with the server. With (t, r) denoting the communication round t and local iteration r , we define $\bar{\mathbf{s}}_k^{(t,0)} = \sum_{i=1}^K \alpha_{k,i}^{(t,0)} \mathbf{s}_i^{(t,0)}$ for $t \in [0, T-1]$ and $r \in [0, \tau-1]$ where $\bar{\mathbf{s}}_k^{(t,0)}$ is fixed for all r and updated only for every t . The term T and τ is the total number of communication rounds and local iterations respectively. Note that the logit information $\bar{\mathbf{s}}_k^{(t,0)}$ is

¹Unlike the majority of existing distillation methods which require expensive labeled data, we show the feasibility of leveraging unlabeled datasets. Note that unlabeled data can be either achieved by existing datasets or a pre-trained generator (e.g., GAN).

computed and sent by the server to the clients for every communication round t . Details are in the following paragraphs and Algorithm 1.

Client Side Update. From (1), given $\bar{s}_k^{(t,0)}$ from the server, each client's local update rule is:

$$\mathbf{w}_k^{(t,r+1)} = \mathbf{w}_k^{(t,r)} - \eta_t \left[\frac{2\lambda}{|\mathcal{P}_k^{(t,r)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t,r)}} \nabla s(\mathbf{w}_k^{(t,r)}, \mathbf{x})^T \left(s(\mathbf{w}_k^{(t,r)}, \mathbf{x}) - \bar{s}_k^{(t,0)}(\mathbf{x}) \right) \right. \quad (2)$$

$$\left. + \frac{1}{|\xi_k^{(t,r)}|} \sum_{\xi \in |\xi_k^{(t,r)}|} \nabla f(\mathbf{w}_k^{(t,r)}, \xi) \right] \\ \triangleq \mathbf{w}_k^{(t,r)} - \eta_t \mathbf{g}_k(\mathbf{w}_k^{(t,r)}; \bar{s}_k^{(t,0)}) \quad (3)$$

The term $\mathbf{w}_k^{(t,r)}$ denotes the local model parameters of client k , η_t is the learning rate, $\xi_k^{(t,r)}$ is the mini-batch randomly sampled from client k 's local dataset \mathcal{B}_k , and $\mathcal{P}_k^{(t,r)}$ is the mini-batch randomly sampled from the public dataset from client k . We also denote the updated local model of client k after all τ local iterations for round t as $\mathbf{w}_k^{(t+1,0)} = \mathbf{w}_k^{(t,\tau)}$.

For PERFED-CKT, we consider partial client participation where for every communication round t , m clients are selected with probability p_k without replacement from $k \in [K]$. We denote the set of selected clients as $\mathcal{S}^{(t,0)}$ that is fixed for all local iterations $r \in [0, \tau - 1]$. If a client $k \in [K]$ was most recently selected in the previous communication round $t' < t$, and selected again for the current communication round t , we assume that $\mathbf{w}_k^{(t,0)} = \mathbf{w}_k^{(t',\tau)}$. In other words, we retrieve the most recently updated local model for the client that is selected for the next communication round and use that model for local training. Each client $k \in \mathcal{S}^{(t,0)}$ takes $\tau \geq 1$ local updates before sending its logits back to the server where each local update step follows the update in (2).

Server Side Clustered Knowledge Aggregation. After the τ local iterations, each client $k \in \mathcal{S}^{(t,0)}$ sends the logits from its updated local model to the server. The logits are denoted as $\mathbf{s}_k^{(t+1,0)} \in \mathbb{R}^{|\mathcal{P}| \times N}$ which is $s(\mathbf{w}_k^{(t+1,0)}, \mathbf{x}) = s(\mathbf{w}_k^{(t,\tau)}, \mathbf{x}) \in \mathbb{R}^{1 \times N}$ stacked in to rows for each $\mathbf{x} \in \mathcal{P}$. The server uses c -means clustering (also known conventionally as the k -means clustering algorithm [48]) to cluster the received m different set of logits, $\mathbf{s}_k^{(t+1,0)}, k \in \mathcal{S}^{(t)}$ to c clusters, where c is an integer such that $1 \leq c \leq m$. The server also gets the next set of selected clients $\mathcal{S}^{(t+1,0)}$ and sends the centroids $\{\mathbf{c}_i^{(t+1,0)}\}_{i \in [c]}$ for each cluster to the clients in $\mathcal{S}^{(t+1,0)}$. Each client $k' \in \mathcal{S}^{(t+1,0)}$ then determines the centroid that is closest to its current model's logit as

$$\bar{s}_{k'}^{(t+1,0)} = \arg \min_{\{\mathbf{c}_i^{(t+1,0)}\}_{i \in [c]}} \|\mathbf{c}_i^{(t+1,0)} - \mathbf{s}_{k'}^{(t+1,0)}\|_2^2 \quad (4)$$

and uses it for the local update in (2). Since we defined $\bar{s}_{k'}^{(t+1,0)} = \sum_{i=1}^K \alpha_{k',i}^{(t+1,0)} \mathbf{s}_i^{(t+1,0)}$, (4) gives a natural selection of $\alpha_{k',i}^{(t+1,0)}$ which gives higher weight to the $\mathbf{s}_i^{(t+1,0)}$, $i \in \mathcal{S}^{(t,0)}$ that is closer to client k' 's logits, i.e., $\mathbf{s}_i^{(t+1,0)}$. PERFED-CKT can set $\alpha_{k,i} = 0$ for client i if its logit is significantly different from the logit of client k or if it was not included in the previous set of selected clients.

We show in the subsequent sections that our proposed PERFED-CKT indeed converges and improves the generalization performance of the individual clients' personalized models by clustering. We also empirically show that PERFED-CKT achieves high test accuracy as state-of-the-art (SOTA) personalized FL algorithms with drastically smaller communication cost.

4 Theoretical Analysis of PERFED-CKT

In this section, we analyze the convergence and generalization properties of PERFED-CKT, specifically highlighting the effect of clustered knowledge transfer to generalization.

Algorithm 1 Personalized Federated Learning with Clustered Knowledge Transfer (PERFED-CKT)

- 1: **Input:** $m, \{p_k\}_{k \in [K]}$, mini-batch size b, b' for private, public data each, number of clusters c
 - 2: **Output:** $\{\mathbf{w}_k\}_{k \in [K]}$
 - 3: **Initialize:** $\{\mathbf{s}_k^{(0,0)}\}_{k \in \mathcal{S}^{(-1,0)}}$, selected set of m clients $\mathcal{S}^{(-1,0)}$
 - 4: **For** $t = 0, \dots, T - 1$ **communication rounds do:**
 - 5: **Global server do:**
 - 6: Cluster $\{\mathbf{s}_k^{(t,0)}\}_{k \in \mathcal{S}^{(t-1,0)}}$ by c -means clustering
 - 7: Get centroids $\{\mathbf{c}_i^{(t,0)}\}_{i \in [c]}$ for each cluster
 - 8: Select m clients for $\mathcal{S}^{(t,0)}$ without replacement from $[K]$ by the dataset ratio $\{p_k\}_{k \in [K]}$
 - 9: Send centroids $\{\mathbf{c}_i^{(t,0)}\}_{i \in [c]}$ to clients $k \in \mathcal{S}^{(t,0)}$
 - 10: **Clients $k \in \mathcal{S}^{(t,0)}$ in parallel do:**
 - 11: Get $\mathbf{s}_k^{(t,0)}$ for current local model $\mathbf{w}_k^{(t,0)}$, and find $\bar{\mathbf{s}}_k^{(t,0)} = \arg \min_{\{\mathbf{c}_i^{(t,0)}\}_{i \in [c]}} \|\mathbf{c}_i^{(t,0)} - \mathbf{s}_k^{(t,0)}\|_2^2$.
 - 12: **For** $r = 0, \dots, \tau - 1$ **local iterations do:**
 - 13: Create mini-batch $\xi_k^{(t,r)}$ from sampling b samples uniformly at random from \mathcal{B}_k , and mini-batch $\mathcal{P}_k^{(t,r)}$ from sampling b' samples uniformly at random from \mathcal{P}
 - 14: Update $\mathbf{w}_k^{(t,r+1)} \leftarrow \mathbf{w}_k^{(t,r)} - \eta \mathbf{g}_k(\mathbf{w}_k^{(t,r)}; \bar{\mathbf{s}}_k^{(t,0)})$
 - 15: Send $\mathbf{s}_k^{(t+1,0)} = \mathbf{s}_k^{(t,\tau)}$ for the updated local model $\mathbf{w}_k^{(t,\tau)}$ back to the server
-

Convergence Analysis

Here, we present the convergence guarantees of PERFED-CKT with regards to the objective function $\Phi_k(\mathbf{w}_k^{(t,0)}; \bar{\mathbf{s}}_k^{(t,0)})$ as $t \rightarrow \infty$ with $\tau = 1$. We use the following assumptions for our analysis:

Assumption 4.1. *The composite loss function $f(\mathbf{w}, \xi)$ is Lipschitz-continuous and Lipschitz-smooth for all \mathbf{w} , ξ , and therefore $F_1(\mathbf{w}), \dots, F_k(\mathbf{w})$ are all L_f -continuous and L_p -smooth for all \mathbf{w} .*

Assumption 4.2. *Each F_1, \dots, F_k is bounded below by a scalar $F_{k,\inf}$ over its domain for $k \in [K]$.*

Assumption 4.3. *For the mini-batch ξ_k uniformly sampled at random from \mathcal{B}_k , the resulting stochastic gradient is unbiased, that is, $\mathbb{E} \left[\frac{1}{|\xi_k|} \sum_{\xi \in \xi_k} \nabla f(\mathbf{w}_k, \xi) \right] = \nabla F_k(\mathbf{w}_k)$.*

Assumption 4.4. *The stochastic gradient's expected squared norm is uniformly bounded, i.e., $\mathbb{E} \left\| \frac{1}{|\xi_k|} \sum_{\xi \in \xi_k} \nabla f(\mathbf{w}_k, \xi) \right\|^2 \leq G^2$ for $k = 1, \dots, K$.*

Assumption 4.5. *$s(\mathbf{w}, \mathbf{x})$ is L_s -continuous and L_g -smooth for all \mathbf{w} and x .*

Now we present the convergence guarantees for PERFED-CKT in Theorem 4.1 below:

Theorem 4.1. *With Assumption 4.1-Assumption 4.5, after running PERFED-CKT (Algorithm 1) for $t = T$ iterations on client $k \in [K]$ with K total clients participating, with the learning rate satisfying $\sum_{t=0}^{\infty} \eta_t = \infty$, $\sum_{t=0}^{\infty} \eta_t^2 < \infty$, we have that the norm of the gradient of $\Phi_k(\mathbf{w}_k^{(t,0)}; \bar{\mathbf{s}}_k^{(t,0)})$ with respect to $\mathbf{w}_k^{(t,0)}$ given $\bar{\mathbf{s}}_k^{(t,0)}$ goes to zero with probability 1 as $T \rightarrow \infty$, i.e., for every client k ,*

$$\lim_{t \rightarrow \infty} \|\nabla_{\mathbf{w}_k^{(t,0)}} \Phi_k(\mathbf{w}_k^{(t,0)}; \bar{\mathbf{s}}_k^{(t,0)})\| = 0 \quad (5)$$

The proof for Theorem 4.1 is presented in the Appendix A. Theorem 4.1 shows that our proposed algorithm PERFED-CKT indeed converges to a first-order stationary point with respect to \mathbf{w}_k given $\bar{\mathbf{s}}_k$ where the norm of the gradient of our main objective function $\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k)$ with respect to \mathbf{w}_k is 0.

Generalization Performance

Now we show the theoretical grounds for clustered knowledge distillation in regards to the generalization performance for personalized FL in the problem of linear regression. We also present a generalization bound for ensemble models in the context of personalization in Appendix D. For K clients in total, we consider a Bayesian framework as in [25] where we have θ uniformly distributed on \mathbb{R}^d , and each device has its data distributed with parameters $\mathbf{w}_k = \theta + \zeta_k$ where $\zeta_k \sim \mathcal{N}(0, v_k^2 \mathbf{I}_d)$ and \mathbf{I}_d is the $d \times d$ identity matrix and v_k is unique to the client's task. Suppose we have $\mathbf{y}_k = \mathbf{X}_k \mathbf{w}_k + \mathbf{z}$, $k \in [K]$ where $\mathbf{y}_k \in \mathbb{R}^n$, $\mathbf{X}_k \in \mathbb{R}^{n \times d}$, and $\mathbf{z} \in \mathbb{R}^n$ such that $\mathbf{z} \sim \mathcal{N}(0, \sigma^2 \mathbf{I}_d)$.

Let us consider a linear regression problem for each device k such that we have the empirical loss function as $F_k(\mathbf{w}_k) = \|\mathbf{X}_k \mathbf{w}_k - \mathbf{y}_k\|_2^2$. We have that $\hat{\mathbf{w}}_k = (\mathbf{X}_k^T \mathbf{X}_k)^{-1} \mathbf{X}_k^T \mathbf{y}_k$ is a noisy observation of \mathbf{w}_k with additive covariance $\sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1}$ since $\hat{\mathbf{w}}_k \sim \mathcal{N}((\mathbf{X}_k^T \mathbf{X}_k)^{-1} \mathbf{X}_k^T \mathbf{y}_k, \sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1})$. Then using Lemma 2 from [25], with the following definitions:

$$\Sigma_k := \sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1} + v_k^2 \mathbf{I}_d \quad (6)$$

$$\bar{\Sigma}_{\setminus k} = \left(\sum_{i \in [K], i \neq k} \Sigma_i^{-1} \right)^{-1} \quad (7)$$

$$\bar{\theta}_{\setminus k} := \bar{\Sigma}_{\setminus k} \sum_{i \in [K], i \neq k} \Sigma_i^{-1} \hat{\mathbf{w}}_i \quad (8)$$

given $\{\mathbf{X}_i, \mathbf{y}_i\}_{i \in [K], i \neq k}$ we have that

$$\theta = \bar{\theta}_{\setminus k} + \gamma \quad (9)$$

where $\gamma \sim \mathcal{N}(0, \bar{\Sigma}_{\setminus k})$. Further, if we let

$$\tilde{\Sigma}_k := \bar{\Sigma}_{\setminus k} + v_k^2 \mathbf{I}_d \quad (10)$$

$$\bar{\Sigma}_k := \left((\tilde{\Sigma}_k)^{-1} + (\sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1})^{-1} \right)^{-1} \quad (11)$$

given $\{\mathbf{X}_i, \mathbf{y}_i\}_{i \in [K]}$, again with Lemma 2 from [25] we have

$$\mathbf{w}_k = \bar{\Sigma}_k (\sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1})^{-1} \hat{\mathbf{w}}_k + \bar{\Sigma}_k (\tilde{\Sigma}_k)^{-1} \bar{\theta}_{\setminus k} + \vartheta_k \quad (12)$$

where $\vartheta_k \sim \mathcal{N}(0, \bar{\Sigma}_k)$. The term for \mathbf{w}_k in (12) uses the fact that $\hat{\mathbf{w}}_k$ is a noisy observation of \mathbf{w}_k with additive noise of zero mean and covariance $\sigma^2 (\mathbf{X}_k^T \mathbf{X}_k)^{-1}$, and $\bar{\theta}_{\setminus k}$ is a noisy observation of θ with covariance $\bar{\Sigma}_{\setminus k}$. Given all the training samples from K devices, \mathbf{w}_k in (12) is Bayes optimal.

With PERFED-CKT, following (1), we solve the following objective:

$$\min_{\mathbf{w}_k} \|\mathbf{X}_k \mathbf{w}_k - \mathbf{y}_k\|_2^2 + \lambda_k \|\bar{\mathbf{s}}_k - s(\mathbf{w}_k)\|_2^2 \quad (13)$$

where λ_k is the regularization term as in (1) and $\bar{\mathbf{s}}_k$ and $s(\mathbf{w}_k)$ each is comparative to the $\bar{\mathbf{s}}_k(\mathbf{x})$ and $s(\mathbf{w}_k, \mathbf{x})$ in (1) for a single public data point \mathbf{x} . Note that in the setting of linear regression we can set $s(\mathbf{w}_k) = \mathbf{P}\mathbf{w}_k$ where $\mathbf{P} \in \mathbb{R}^{1 \times d}$ is the public data (without loss of generality, we assume single data point for the public data for simplicity). Accordingly, we set $\bar{\mathbf{s}}_k = \sum_{i=1}^K \alpha_{k,i} s(\hat{\mathbf{w}}_i)$ for an arbitrary set of weights $\alpha_{k,i}, i \in [K]$ for client k . Then we have that the local empirical risk minimizer for (13) is

$$\tilde{\mathbf{w}}_k = (\mathbf{X}_k^T \mathbf{X}_k + \lambda_k \mathbf{P}^T \mathbf{P})^{-1} (\mathbf{X}_k^T \mathbf{X}_k \hat{\mathbf{w}}_k + \lambda_k \mathbf{P}^T \mathbf{P} \sum_{i=1}^K \alpha_{k,i} \hat{\mathbf{w}}_i) \quad (14)$$

Finally, we present the optimal λ_k^* and $\alpha_{k,i}^*$ for any device $k \in [K]$ given the above linear regression problem with PERFED-CKT in Theorem 4.2.

Theorem 4.2. Assuming $\mathbf{X}_k^T \mathbf{X}_k = \beta \mathbf{I}_d$ and $\mathbf{P}^T \mathbf{P} = \nu \mathbf{I}_d$ for some constant β, ν , the λ_k^* and $\alpha_{k,i}^*, i \in [K]$ that minimizes the test performance on device k , $k \in [K]$ i.e.,

$$\lambda_k^*, \alpha_{k,i}^*, i \in [K] = \arg \min_{\lambda_k, \alpha_{k,i}, i \in [K]} \mathbb{E}[F_k(\tilde{\mathbf{w}}_k) | \hat{\mathbf{w}}_k, \bar{\theta}_{\setminus k}] \quad (15)$$

we have that

$$\lambda_k^* = \sigma^2/v_k^2\nu, \alpha_{k,i}^* = \frac{B_k}{\sigma^2 + \beta v_i^2} \quad (16)$$

with $A_k = \left(\sum_{i \in [K], i \neq k} \frac{1}{\sigma^2 + \beta v_i^2}\right)^{-1}, B_k = \frac{A_k(\sigma^2 + \beta v_k^2)}{\sigma^2 + A_k \beta v_k^2}$.

Theorem 4.2 shows that given the objective function in (13) and the corresponding minimizer (14), in a data-heterogeneous scenario where $v_k, k \in [K]$ is unique to each client k , we have that the optimal weights $\alpha_{k,i}^*, i \in [K]$ for client k is in fact inversely proportional to v_i . Intuitively, this means that since larger v_i leads to a larger divergence from the original θ in $\mathbf{w}_i = \theta + \zeta_i$, giving lower weight $\alpha_{k,i}$ to client i improves generalization of the personalized model. This gives new insight into co-distillation for personalization in FL since previous work [30, 34] only consider scenarios where the weight $\alpha_{i,k} = 1/K, \forall i, k \in [K]$ in a non-personalized FL setting. The results also present strong motivation for clustered knowledge transfer for personalized FL. The proof for Theorem 4.2 is presented in Appendix B. Further discussions on the implications of Theorem 4.2 is presented in Appendix C.

5 Experiments

For all experiments we randomly sample a fraction (C) of clients from $K = 100$ clients per communication round for local training. For the sake of simplicity and fair comparison across different benchmarks, we use do not apply any momentum acceleration or weight decay to local training. Further details of the experimental setup are in Appendix E.

Experimental Setup

Datasets and models. We evaluate PERFED-CKT with CIFAR10 [49] as the training/test dataset and CIFAR100 [50] as the public dataset for image classification in mainly two different scenarios: model homogeneity and heterogeneity. For model homogeneity, VGG11 [51] is deployed for all clients. For model heterogeneity, we sample one of VGG13/VGG11/CNN model architecture for each client with the probability of a larger model getting assigned to a client is proportional to the client’s dataset size (see Figure 2(a)). We partition data heterogeneously amongst clients using the Dirichlet distribution $\text{Dir}_K(\alpha)$ [52], smaller α leads to higher data size imbalance and degree of label skew across clients. We set $\alpha = 0.01$ to emulate realistic FL scenarios with large data-heterogeneity (see Figure 2(b)).

Baselines. We compare PERFED-CKT with SOTA FL algorithms designed to efficiently train either (i) a single global model at the server (e.g. FedAvg, FedProx, Scaffold, FedDF) or (ii) personalized model(s) either at the server side as a global model (GM) or client side (e.g., PerFedAvg, FedFomo, Ditto, HypCluster) as a local model (LM). Note that we do not assume a *labeled* public dataset, and instead relax the condition to a *small*² and *unlabeled* public dataset and therefore exclude comparison to methods which require training directly on a *labeled* public dataset (e.g., FedMD).

Experimental Results

We demonstrate the efficacy of PERFED-CKT in terms of the average test accuracy across all clients with the communication cost defined as the total number of parameters communicated across server/clients during the training process including uplink and downlink.

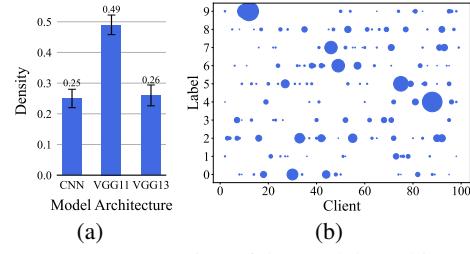


Figure 2: (a) Proportion of the models architectures deployed across clients for the model heterogeneity scenario; (b) data-distribution with $\alpha = 0.01$ for all clients where larger circle indicates larger dataset size for each label 0-9 of CIFAR10.

²We only use 2000 unlabeled data-samples per experiment that are sampled uniformly at random from CIFAR100.

Table 1: Average test accuracy across the entire clients and total communication cost (number of parameters communicated per round) for the model-homogeneous scenario with total number of clients $K = 100$. The standard deviation for the test accuracy across random seeds is shown in the parenthesis.

Method	Algorithm	$C = 0.10$		$C = 0.15$	
		Test Acc.	Com.-Cost	Test Acc.	Com.-Cost
Local Training	-	64.02 (± 0.48)	-	64.02 (± 0.48)	-
	FedAvg	15.53 (± 1.42)		20.00 (± 2.66)	
Non- Personalized	FedProx	13.64 (± 1.23)		16.71 (± 1.79)	
	Scaffold	12.92 (± 1.46)		16.41 (± 1.14)	
	FedDF	15.18 (± 1.18)	2150×10^7	17.09 (± 1.54)	3120×10^7
	Per-FedAvg (GM)	14.47 (± 0.59)		14.61 (± 0.83)	
	Per-FedAvg (LM)	51.74 (± 1.52)		50.25 (± 1.61)	
Personalized	Ditto (LM)	67.21 (± 1.86)		68.88 (± 1.95)	
	Ditto (GM)	21.63 (± 2.13)		19.16 (± 2.34)	
	FedFomo	74.62 (± 0.42)	3900×10^7	77.56 (± 0.75)	5850×10^7
	HypCluster ($c = 2$)	34.11 (± 2.63)	2340×10^7	28.70 (± 3.03)	3320×10^7
	HypCluster ($c = 3$)	39.17 (± 2.64)	2540×10^7	41.99 (± 2.48)	3510×10^7
	HypCluster ($c = 5$)	52.51 (± 1.37)	2930×10^7	51.92 (± 1.64)	3900×10^7
	HypCluster ($c = 6$)	65.77 (± 2.76)	3120×10^7	63.28 (± 1.16)	4100×10^7
	PERFED-CKT ($c = 1$)	70.70 (± 0.46)	4.4×10^7	67.66 (± 0.30)	6.4×10^7
	PERFED-CKT ($c = 2$)	73.33 (± 0.26)	4.8×10^7	70.86 (± 0.73)	6.8×10^7
	PERFED-CKT ($c = 3$)	74.31 (± 0.40)	5.2×10^7	76.74 (± 0.71)	7.2×10^7
	PERFED-CKT ($c = 4$)	72.67 (± 0.31)	5.6×10^7	73.52 (± 1.15)	7.6×10^7

Table 2: Average test accuracy across all clients and total communication cost (number of parameters communicated per round) for the model-heterogeneous scenario with total number of clients $K = 100$. The standard deviation for the test accuracy across random seeds is shown in the parenthesis.

Method	Algorithm	$C = 0.10$		$C = 0.15$	
		Test Acc.	Com.-Cost	Test Acc.	Com.-Cost
Local Training	-	59.29 (± 1.05)	-	59.29 (± 1.05)	-
Non-Personalized	FedDF	15.25 (± 1.21)	1780×10^7	14.16 (± 1.11)	2620×10^7
Personalized	PERFED-CKT ($c = 1$)	70.94 (± 0.46)	4.4×10^7	70.77 (± 0.14)	6.4×10^7
	PERFED-CKT ($c = 2$)	72.25 (± 0.17)	4.8×10^7	76.14 (± 0.73)	6.8×10^7
	PERFED-CKT ($c = 3$)	71.84 (± 0.40)	5.2×10^7	76.02 (± 0.66)	7.2×10^7
	PERFED-CKT ($c = 4$)	70.01 (± 0.31)	5.6×10^7	73.14 (± 0.61)	7.6×10^7

Test Accuracy and Communication Cost. In Table 1, we show the performance of PERFED-CKT along with the performance of other SOTA FL algorithms in regards to the achieved highest test accuracy and communicated number of parameters between server and client with different fractions of selected clients C . For $C = 0.1$, we show that PERFED-CKT achieves high test accuracy of 74.31% with $c = 3$, with small communication cost compared to other algorithms (saving at maximum $\times 750$). FedFomo achieves a slightly higher test accuracy performance with 74.62%, but the communication cost spent, 3900×10^7 parameters, is significantly larger compared to PERFED-CKT which is 5.2×10^7 parameters. Moreover note that algorithms that train a single global model in the non-personalized FL setting performs worse than personalized algorithms showing that the traditional FL framework does not perform well to individual clients in the setting of high data heterogeneity. For $C = 0.15$, we also show that PERFED-CKT is able to achieve a comparable high test accuracy of 76.74% with only a small communication cost of 7.2×10^7 parameters (saving at maximum $\times 812.5$) where FedFomo achieves a slightly higher accuracy of 77.56% with large communication cost of 5850×10^7 .

Model Heterogeneity. We demonstrate the performance of PERFED-CKT where clients have different models dependent on their dataset size (see Figure 2(b)) in Table 2. Note that this is a

realistic setting of FL where clients can have smaller or larger models dependent on their dataset size or system capabilities. Only FedDF is capable for model heterogeneity amongst the SOTA FL algorithms which we included for comparison. With model heterogeneity, PERFED-CKT achieves high test accuracy 72.25% for $C = 0.1$ and 76.14% for $C = 0.15$ with even smaller communication cost of 4.8×10^7 and 6.8×10^7 respectively. For $C = 0.15$, the test accuracy is close to that of PERFED-CKT for model homogeneity, showing that allowing model heterogeneity increases feasibility while not hurting the local performance of clients.

Effect of Clustering. PERFED-CKT performs clustering at the server side to cluster the logit information received from the clients. We evaluate how the number of clusters effects the test accuracy and communication cost. For both $C = 0.1$ and $C = 0.15$ in Table 1, $c = 3$ achieves the best test accuracy performance. Increasing c from that point actually deteriorates the performance with higher communication cost. This shows that while clustering can help to a certain extent, too much clustering can hurt generalization since we are decreasing the number of clients in each cluster and the diversity of information within each cluster. Similar behavior is observed in Table 1 where the best test accuracy is achieved in $c = 2$, and then the accuracy decreases for higher c .

6 Concluding Remarks

The inherently high data and system heterogeneity across resource-constrained clients in FL should be considered for devising realistic personalized FL schemes. However, previous work in personalized FL restricted clients to have homogeneous models across clients with direct communication of the model parameters which can incur heavy communication cost. We propose PERFED-CKT that caters to the data and system heterogeneity across clients by using clustered knowledge transfer, allowing heterogeneous model deployment without direct communication of the models. We show that PERFED-CKT achieves competitive performance compared to other SOTA personalized FL schemes at a much smaller communication cost. Interesting future directions of this work include understanding the privacy implications that arise due to the clustering of clients and communicating their logits instead of the actual model parameters.

References

- [1] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agøura y Arcas. Communication-Efficient Learning of Deep Networks from Decentralized Data. *International Conference on Artificial Intelligence and Statistics (AISTATS)*, April 2017.
- [2] Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurelien Bellet, Mehdi Benni, Arjun Nitin Bhagoji, Keith Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, Rafael G. L. D’Oliveira, Salim El Rouayheb, David Evans, Josh Gardner, Zachary Garrett, Adria Gascon, Badih Ghazi, Phillip B. Gibbons, Marco Gruteser, Zaid Harchaoui, Chaoyang He, Lie He, Zhouyuan Huo, Ben Hutchinson, Justin Hsu, Martin Jaggi, Tara Javidi, Gauri Joshi, Mikhail Khodak, Jakub Konecny, Aleksandra Korolova, Farinaz Koushanfar, Sanmi Koyejo, Tancrede Lepoint, Yang Liu, Prateek Mittal, Mehryar Mohri, Richard Nock, Ayfer Ozgur, Rasmus Pagh, Mariana Raykova, Hang Qi, Daniel Ramage, Ramesh Raskar, Dawn Song, Weikang Song, Sebastian U. Stich, Ziteng Sun, Ananda Theertha Suresh, Florian Tramer, Praneeth Vepakomma, Jianyu Wang, Li Xiong, Zheng Xu, Qiang Yang, Felix X. Yu, Han Yu, and Sen Zhao. Advances and open problems in federated learning. *arXiv preprint arXiv:1912.04977*, 2019.
- [3] Keith Bonawitz, Hubert Eichner, Wolfgang Grieskamp, Dzmitry Huba, Alex Ingberman, Vladimir Ivanov, Chloe Kiddon, Jakub Konecny, Stefano Mazzocchi, H. Brendan McMahan, Timon Van Overveldt, David Petrou, Daniel Ramage, and Jason Roslander. Towards Federated Learning at Scale: System Design. *SysML*, April 2019.
- [4] Jianyu Wang, Zachary Charles, Zheng Xu, Gauri Joshi, H Brendan McMahan, Maruan Al-Shedivat, Galen Andrew, Salman Avestimehr, Katharine Daly, Deepesh Data, et al. A field guide to federated optimization. *arXiv preprint arXiv:2107.06917*, 2021.
- [5] Hao Yu, Sen Yang, and Shenghuo Zhu. Parallel restarted SGD for non-convex optimization with faster convergence and less communication. *The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19)*, 2019.
- [6] Sebastian U Stich. Local SGD converges fast and communicates little. In *International Conference on Learning Representations (ICLR)*, 2019.
- [7] Jianyu Wang and Gauri Joshi. Cooperative SGD: A unified framework for the design and analysis of communication-efficient SGD algorithms. *Journal of Machine Learning Research (JMLR)*, 2021.
- [8] Yae Jee Cho, Jianyu Wang, and Gauri Joshi. Client selection in federated learning: Convergence analysis and power-of-choice selection strategies. *abs/2010.01243*, 2020.
- [9] Sashank Reddi, Zachary Charles, Manzil Zaheer, Zachary Garrett, Keith Rush, Jakub Konečný, Sanjiv Kumar, and H Brendan McMahan. Adaptive federated optimization. In *International Conference on Learning Representations (ICLR)*, 2021.
- [10] Farzin Haddadpour and Mehrdad Mahdavi. On the convergence of local descent methods in federated learning. *arXiv preprint arXiv:1910.14425*, 2019.
- [11] A Khaled, K Mishchenko, and P Richtárik. Tighter theory for local SGD on identical and heterogeneous data. In *The 23rd International Conference on Artificial Intelligence and Statistics (AISTATS 2020)*, 2020.
- [12] Sebastian U Stich and Sai Praneeth Karimireddy. The error-feedback framework: Better rates for SGD with delayed gradients and compressed communication. *Journal of Machine Learning Research (JMLR)*, 2020.
- [13] Blake Woodworth, Kumar Kshitij Patel, Sebastian U Stich, Zhen Dai, Brian Bullins, H Brendan McMahan, Ohad Shamir, and Nathan Srebro. Is local SGD better than minibatch SGD? In *Proceedings of the 37th International Conference on Machine Learning*, 2020.
- [14] Anastasia Koloskova, Nicolas Loizou, Sadra Boreiri, Martin Jaggi, and Sebastian U Stich. A unified theory of decentralized SGD with changing topology and local updates. In *Proceedings of 37th International Conference on Machine Learning*, 2020.

- [15] Zhouyuan Huo, Qian Yang, Bin Gu, Lawrence Carin, and Heng Huang. Faster on-device training using new federated momentum algorithm. *arXiv preprint arXiv:2002.02090*, 2020.
- [16] Xinwei Zhang, Mingyi Hong, Sairaj Dhople, Wotao Yin, and Yang Liu. FedPD: A federated learning framework with optimal rates and adaptivity to non-IID data. *Asilomar Conference on Signals, Systems, and Computers.*, 2020.
- [17] Reese Pathak and Martin J Wainwright. FedSplit: An algorithmic framework for fast federated optimization. In *Advances in Neural Information Processing Systems*, 2020.
- [18] Grigory Malinovsky, Dmitry Kovalev, Elnur Gasanov, Laurent Condat, and Peter Richtárik. From local SGD to local fixed point methods for federated learning. In *Proceedings of the 37th International Conference on Machine Learning*, 2020.
- [19] Anit Kumar Sahu, Tian Li, Maziar Sanjabi, Manzil Zaheer, Ameet Talwalkar, and Virginia Smith. Federated optimization for heterogeneous networks. In *Proceedings of the 3rd MLSys Conference*, January 2020.
- [20] Paul Pu Liang, Terrance Liu, Liu Ziyin, , Nicholas B. Allen, Randy P. Auerbach, David Brent, Ruslan Salakhutdinov, and Louis-Philippe Morency. Think locally, act globally: Federated learning with local and global representations. In *International Workshop on Federated Learning for User Privacy and Data Confidentiality inConjunction with NeurIPS 2019 (FL-NeurIPS'19)*, 2019.
- [21] Avishek Ghosh, Jichan Chung, Dong Yin, and Kannan Ramchandran. An efficient framework for clustered federated learning. In *Advances in Neural Information Processing Systems*, 2020.
- [22] Alysa Ziying Tan, Han Yu, Lizhen Cui, and Qiang Yang. Towards personalized federated learning. *CoRR*, abs/2103.00710, 2020.
- [23] Alireza Fallah, Aryan Mokhtari, and Asuman Ozdaglar. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. In *Advances in Neural Information Processing Systems*, 2020.
- [24] M. Zhang, K. Sapra, S. Fidler, S. Yeung, and J. M. Alvarez. Personalized federated learning with first order model optimization. In *International Conference on Learning Representations (ICLR)*, 2021.
- [25] Tian Li, Shengyuan Hu, Ahmad Beirami, and Virginia Smith. Ditto: Fair and robust federated learning through personalization. In *Proceedings of the 38th International Conference on Machine Learning*, 2021.
- [26] Yishay Mansour, Mehryar Mohri, Jae Ro, and Ananda Theertha Suresh. Three approaches for personalization with applications to federated learning. *arXiv preprint cs.LG 2002.10619*, 2020.
- [27] Noam Shazeer, Azalia Mirhoseini, Krzysztof Maziarz, Andy Davis, Quoc V. Le, Geoffrey E. Hinton, and Jeff Dean. Outrageously large neural networks: The sparsely-gated mixture-of-experts layer. In *International Conference on Learning Respresentations (ICLR)*, 2017.
- [28] Chaoyang He, Murali Annaram, and Salman Avestimehr. Group knowledge transfer: Federated learning of large cnns at the edge. In *Advances in Neural Information Processing Systems*, 2020.
- [29] S. Sodhani, O. Delalleau, M. Assran, K. Sinha, N. Ballas, and M. Rabbat. A closer look at codistillation for distributed training. *CoRR*, abs/2010.02838, 2020.
- [30] I. Bistrizt, A. J. Mann, and N. Bambos. Distributed distillation for on-device learning. In *Advances in Neural Information Processing Systems*, 2020.
- [31] Tao Lin, Lingjing Kong, Sebastian U. Stich, and Martin Jaggi. Ensemble distillation for robust model fusion in federated learning. In *Advances in Neural Information Processing Systems*, 2020.

- [32] Rohan Anil, Gabriel Pereyra, Alexandre Passos, Robert Ormandi, George E. Dahl, and Geoffrey E. Hinton. Large scale distributed neural network training through online distillation. In *International Conference on Learning Representations (ICLR)*, 2018.
- [33] Canh T. Dinh, Nguten H. Tran, and Tuan Dung Nguyen. Personalized federated learning with moreau envelopes. In *Advances in Neural Information Processing Systems*, 2020.
- [34] Daliang Li and Junpu Wang. Fedmd: Heterogenous federated learning via model distillation. In *International Workshop on Feder-ated Learning for User Privacy and Data Confidentiality inConjunction with NeurIPS 2019 (FL-NeurIPS'19)*, 2019.
- [35] Geoffrey Hinton, Oriol Vinyals, and Jeff Dean. Distilling the knowledge in a neural network. *ArXiv*, March 2015.
- [36] Jiaxin Ma, Ryo Yonetani, and Zahid Iqbal. Adaptive distillation for decentralized learning from heterogeneous clients. In *2020 25th International Conference on Pattern Recognition (ICPR)*, August 2020.
- [37] Sohei Itahara, Takayuki Nishio, Yusuke Koda, Masahiro Morikura, and Koji Yamamoto. Distillation-based semi-supervised federated learning for communication-efficient collaborative training with non-iid private data. *IEEE Transactions on Mobile Computing*, August 2020.
- [38] Lichao Sun and Lingjuan Lyu. Federated model distillation with noise-free differential privacy. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence (IJCAI-21)*, May 2021.
- [39] Qinbin Li, Bingsheng He, and Dawn Song. Practical one-shot federated learning for cross-silo setting. In *Proceedings of the Thirtieth International Joint Conference on Artificial Intelligence (IJCAI-21)*, May 2021.
- [40] Yanlin Zhou, George Pu, Xiyao Ma, Xiaolin Li, and Dapeng Wu. Distilled one-shot federated learning. *ArXiv*, June 2021.
- [41] Sangho Lee, Kiyoon Yoo, and Nojun Kwak. Edge bias in federated learning and its solution by buffered knowledge distillation. *ArXiv*, February 2021.
- [42] Eunjeong Jeong, Seungeun Oh, Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. *International Workshop on Machine Learning on the Phone and other Consumer Devices in Conjunction with NeurIPS (NeurIPS-MLPCD)*, 2018.
- [43] X. Lan, X. Zhu, and S. Gong. Knowledge distillation by on-the-fly native ensemble. In *Proceedings of the 32nd International Conference on Neural Information Processing Systems.*, pages 7528–7538, 2018.
- [44] Lingjuan Lyu, Han Yu, Xingjun Ma, Lichao Sun, Jun Zhao, Qiang Yang, and Philip S. Yu. Privacy and robustness in federated learning: Attacks and defenses. *arXiv preprint arXiv:2012.06337*, 2020.
- [45] Y. Zhang, T. Xiang, T. M. Hospedales, and H. Lu. Deep mutual learning. In *In IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, page 4320–4328, 2018.
- [46] Haoran Zhang, Zhenzhen Hu, Wei Qin, Mingliang Xu, and Meng Wang. Adversarial co-distillation learning for image recognition. *Pattern Recognition*, 111:107659, 2021.
- [47] Xinyang Lin, , Hanting Chen, Yixing Xu, Chao Xu, Xiaolin Gui, Yiping Deng, and Yunhe Wang. Federated Learning with Positive and Unlabeled Data. *preprint*, 2021.
- [48] J. A. Hartigan and M. A. Wong. Algorithm as 136: A k-means clustering algorithm. *Journal of the Royal Statistical Society. Series C (Applied Statistics)*, 28(1):100–108, 1979.
- [49] Alex Krizhevsky, Vinod Nair, and Geoffrey Hinton. Learning multiple layers of features from tiny images. *CIFAR-10 (Canadian Institute for Advanced Research)*, 2009.

- [50] Alex Krizhevsky, Vinod Nair, and Geoffrey Hinton. Cifar-100 (canadian institute for advanced research). <http://www.cs.toronto.edu/~kriz/cifar.html>, 2009.
- [51] Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. In *International Conference on Learning Representations (ICLR)*, 2015.
- [52] Tzu-Ming Harry Hsu, Hang Qi, and Matthew Brown. Measuring the effects of non-identical data distribution for federated visual classification. In *International Workshop on Federated Learning for User Privacy and Data Confidentiality in Conjunction with NeurIPS 2019 (FL-NeurIPS'19)*, December 2019.
- [53] Tomaso Poggio, Stephen Voinea, and Lorenzo Rosasco. Online learning, stability, and stochastic gradient descent, 2019.
- [54] Ya.I. Alber, A.N. Iusem, and M.V. Solodovz. On the projected subgradient method for non-smooth convex optimization in a hilbert space. *Mathematical Programming*, 81(1):23–25, 1998.
- [55] S. Ben-David, J. Blitzer, K. Crammer, A. Kulesza, F. Pereira, and J. W. Vaughan. A theory of learning from different domains. *Machine Learning*, 79(1-2):151–175, 2009.

A Proof for Theorem 4.1

In this section we present the proof for Theorem 4.1. We follow the techniques presented by [30] for the proof. For notational simplicity, we note all super subscript $(t, 0)$ as (t) throughout the proof, dropping the local iteration index. We define the following σ -algebra on the set that contains the history of the model updates for all clients with $\mathbf{w}^{(t)} = [\mathbf{w}_1^{(t)} \dots \mathbf{w}_K^{(t)}]$ and $\bar{\mathbf{s}}^{(t)} = [\bar{\mathbf{s}}_1^{(t)} \dots \bar{\mathbf{s}}_K^{(t)}]$ as $\mathcal{H}_t = \sigma(\{\mathbf{w}^{(i)}, \bar{\mathbf{s}}^{(i)}\} \mid i \leq t)$. Recall $\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) \triangleq \frac{1}{|\xi_k^{(t)}|} \sum_{\xi \in \xi_k^{(t)}} \nabla f(\mathbf{w}_k^{(t)}, \xi) + \frac{2\lambda}{|\mathcal{P}_k^{(t)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t)}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x}))$.

Additional Lemmas

We first present useful Lemmas and their proofs which we use for the intermediate steps in the main proof for Theorem 4.1.

Lemma A.1. *The gradient of the second term in $\Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})$ with respect to $\mathbf{w}_k^{(t)}$ is Lipschitz continuous, and therefore with assumption 4.1, $\Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})$ is also a Lipschitz-smooth function with factor L_p .*

Proof. With dropping the iteration index t for the upper script for simplicity, let's define the second term in $\Phi_k(\mathbf{w}_k; \bar{\mathbf{s}}_k)$ as $q(\mathbf{w}_k; \bar{\mathbf{s}}_k) \triangleq \frac{\lambda}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \|\bar{\mathbf{s}}(\mathbf{x}) - s(\mathbf{w}_k, \mathbf{x})\|_2^2$. Then we have that

$$\nabla_{\mathbf{w}_k} q(\mathbf{w}_k; \bar{\mathbf{s}}_k) = \frac{2\lambda}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{w}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})) \quad (17)$$

For an arbitrary \mathbf{e}_k in the domain of $q(\cdot; \bar{\mathbf{s}}_k)$ for each $\mathbf{x} \in \mathcal{P}$, we have that

$$\begin{aligned} & \|\nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{w}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})) - \nabla s(\mathbf{e}_k, \mathbf{x})^T (s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x}))\|^2 \\ & \leq 3\|\nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{w}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})) - \nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x}))\|^2 \end{aligned} \quad (18)$$

$$\begin{aligned} & + 3\|\nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})) - \nabla s(\mathbf{e}_k, \mathbf{x})^T (s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x}))\|^2 \\ & \leq 3\|\nabla s(\mathbf{w}_k, \mathbf{x})\|^2 \|s(\mathbf{w}_k, \mathbf{x}) - s(\mathbf{e}_k, \mathbf{x})\|^2 + 3\|\nabla s(\mathbf{w}_k, \mathbf{x}) - \nabla s(\mathbf{e}_k, \mathbf{x})\|^2 \|s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})\|^2 \end{aligned} \quad (19)$$

$$\leq 3L_s^4 \|\mathbf{w}_k - \mathbf{e}_k\|^2 + 6L_g^2 \|\mathbf{w}_k - \mathbf{e}_k\|^2 \quad (20)$$

$$= (3L_s^4 + 6L_g^2) \|\mathbf{w}_k - \mathbf{e}_k\|^2 \quad (21)$$

where (18) uses Jensen's inequality for the ℓ_2 -norm for three terms, (19) uses the submultiplicativity of the norm, and the LHS of (20) uses assumption 4.5. Therefore we can conclude that $\|\nabla s(\mathbf{w}_k, \mathbf{x})^T (s(\mathbf{w}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x})) - \nabla s(\mathbf{e}_k, \mathbf{x})^T (s(\mathbf{e}_k, \mathbf{x}) - \bar{\mathbf{s}}_k(\mathbf{x}))\|^2$ for any \mathbf{x} is Lipschitz-continuous, and hence $\nabla_{\mathbf{w}_k} q(\mathbf{w}_k; \bar{\mathbf{s}}_k)$ is also Lipschitz-continuous. \square

Lemma A.2. *We have that $\mathbb{E}[\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) | \mathcal{H}_t] = \nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})$ and $\mathbb{E}[\|\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|_2^2] \leq 2G^2 + 16\lambda^2 L_s^2$ and $\|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|$ and $\|\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|$ is each bounded by constant $M_1 \geq 0$ and $M_2 \geq 0$.*

Proof. By definition of the gradient we have

$$\begin{aligned} & \mathbb{E}[\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) | \mathcal{H}_t] \\ & = \mathbb{E}\left[\frac{1}{|\xi_k^{(t)}|} \sum_{\xi \in \xi_k^{(t)}} \nabla f(\mathbf{w}_k^{(t)}, \xi) + \frac{2\lambda}{|\mathcal{P}_k^{(t)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t)}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})) \mid \mathcal{H}_t\right] \end{aligned} \quad (22)$$

$$= \nabla F_k(\mathbf{w}_k^{(t)}) + \frac{2\lambda}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})) \quad (23)$$

$$= \nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) \quad (24)$$

finishing the proof for the first part of lemma A.2. Next, we prove the second part of lemma A.2 showing that

$$\begin{aligned} & \mathbb{E}[\|\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|^2] \\ &= \mathbb{E}\left[\left\|\frac{1}{|\xi_k^{(t)}|} \sum_{\xi \in \xi_k^{(t)}} \nabla f(\mathbf{w}_k^{(t)}, \xi) + \frac{2\lambda}{|\mathcal{P}_k^{(t)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t)}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x}))\right\|^2\right] \end{aligned} \quad (25)$$

$$\begin{aligned} &\leq 2\mathbb{E}\left[\left\|\frac{1}{|\xi_k^{(t)}|} \sum_{\xi \in \xi_k^{(t)}} \nabla f(\mathbf{w}_k^{(t)}, \xi)\right\|^2\right] + 2\mathbb{E}\left[\left\|\frac{2\lambda}{|\mathcal{P}_k^{(t)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t)}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x}))\right\|^2\right] \end{aligned} \quad (26)$$

$$\leq \mathbb{E}\left[\frac{8\lambda^2}{|\mathcal{P}_k^{(t)}|} \sum_{\mathbf{x} \in \mathcal{P}_k^{(t)}} \|\nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x}))\|^2\right] + 2G^2 \quad (27)$$

$$\leq \frac{8\lambda^2}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \mathbb{E}[\|\nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})\|^2 \|s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})\|^2] + 2G^2 \quad (28)$$

$$\leq 2G^2 + 16\lambda^2 L_s^2 \quad (29)$$

where (26) is due to the Cauchy–Schwarz inequality and AM-GM inequality, (27) is due to assumption 4.4 and Jensen’s inequality, (28) is due to the submultiplicativity of the norm, and (29) is due to assumption 4.5 and that the maximum ℓ_2 -norm distance between two probability vectors is $\sqrt{2}$.

Moreover,

$$\|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\| = \left\|\frac{2\lambda}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})) + \nabla F_k(\mathbf{w}_k^{(t)})\right\| \quad (30)$$

$$\leq \frac{2\lambda}{|\mathcal{P}|} \left\| \sum_{\mathbf{x} \in \mathcal{P}} \nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})) \right\| + \|\nabla F_k(\mathbf{w}_k^{(t)})\| \quad (31)$$

$$\leq L_f + 2\lambda \sum_{\mathbf{x} \in \mathcal{P}} \|\nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})^T (s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x}))\| \quad (32)$$

$$\leq L_f + 2\lambda \sum_{\mathbf{x} \in \mathcal{P}} \|\nabla s(\mathbf{w}_k^{(t)}, \mathbf{x})\| \|s(\mathbf{w}_k^{(t)}, \mathbf{x}) - \bar{\mathbf{s}}_k^{(t)}(\mathbf{x})\| \quad (33)$$

$$\leq L_f + 2\sqrt{2}\lambda L_s |\mathcal{P}| = M_1 \quad (34)$$

and therefore $\|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|$ is bounded by $M_1 \geq 0$. With similar steps we can show that $\|\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\| \leq M_2$ for a certain constant $M_2 \geq 0$. \square

Main Proof for Theorem 4.1

Using Lemma A.1 and Lemma A.2 we have that

$$\mathbb{E}[\Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)}) | \mathcal{H}_t] = \mathbb{E}[\Phi_k(\mathbf{w}_k^{(t)} - \eta_t \mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}); \bar{\mathbf{s}}_k^{(t)}) | \mathcal{H}_t] \quad (35)$$

$$\leq \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) + \frac{\eta_t^2 L_p}{2} \mathbb{E}[\|\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|^2 | \mathcal{H}_t] - \eta_t \nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})^T \mathbb{E}[\mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) | \mathcal{H}_t] \quad (36)$$

$$\leq \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)}) - \eta_t \|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|^2 + \frac{\eta_t^2 L_p}{2} (2G^2 + 16\lambda^2 L_s^2) \quad (37)$$

Assuming $\sum_{t=0}^{\infty} \eta_t^2 < \infty$ and $\sum_{t=0}^{\infty} \eta_t = \infty$, and applying Robbins-Siegmund Theorem (Theorem B.1. in [53]) on (37), we have that with probability 1,

$$\sum_{t=1}^{\infty} \eta_t \|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|^2 < \infty \quad (38)$$

Now we can show

$$\|\nabla \Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)})\|^2 - \|\nabla \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|^2 \quad (39)$$

$$= (\|\nabla \Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)})\| + \|\nabla \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|)(\|\nabla \Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)})\| - \|\nabla \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|) \quad (40)$$

$$\leq 2M_1(\|\nabla \Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)})\| - \|\nabla \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\|) \quad (41)$$

$$\leq 2M_1\|\nabla \Phi_k(\mathbf{w}_k^{(t+1)}; \bar{\mathbf{s}}_k^{(t)}) - \nabla \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\| \quad (42)$$

$$\leq 2M_1\|\eta_t \mathbf{g}_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\| \leq 2M_1 M_2 \eta_t \quad (43)$$

Finally, using Proposition 2 in [54] we have that for $t \rightarrow \infty$, $\|\nabla_{\mathbf{w}_k^{(t)}} \Phi_k(\mathbf{w}_k^{(t)}; \bar{\mathbf{s}}_k^{(t)})\| \rightarrow 0$ with probability 1.

B Proof for Theorem 4.2

We have that (13) is equal to:

$$\tilde{\mathbf{w}}_k = \frac{1}{1 + \lambda\nu/\beta} \hat{\mathbf{w}}_k + \frac{1}{1 + \beta/\lambda\nu} \sum_{i=1}^K \alpha_{k,i} \hat{\mathbf{w}}_i \quad (44)$$

and the Bayes optimal \mathbf{w}_k in (12) becomes

$$\mathbf{w}_k = \frac{1}{1 + \sigma^2/\beta v_k^2} \hat{\mathbf{w}}_k + \frac{A_k \sigma^2}{\sigma^2 + A_k \beta v_k^2} \sum_{i=1}^K \frac{1}{\sigma^2 + \beta v_i^2} \hat{\mathbf{w}}_i + \varsigma_k \quad (45)$$

where $A_k = \left(\sum_{i \in [K], i \neq k} \frac{1}{\sigma^2 + \beta v_i^2} \right)^{-1}$ and $\varsigma_k \sim \mathcal{N}\left(0, \left(\frac{\beta}{A_k + \beta v_k^2} + \frac{\beta}{\sigma^2}\right)^{-1}\right)$. If we aim to find the λ_k and $\alpha_{k,i}, i \in [K]$ that minimizes $\mathbb{E}[F_k(\tilde{\mathbf{w}}_k)]$ given $\hat{\mathbf{w}}_k$ and $\bar{\theta}_{\setminus k}$, in other words,

$$\lambda_k^*, \alpha_{k,i}^*, i \in [K] = \arg \min_{\lambda_k, \alpha_{k,i}, i \in [K]} \mathbb{E}[F_k(\tilde{\mathbf{w}}_k) | \hat{\mathbf{w}}_k, \bar{\theta}_{\setminus k}] \quad (46)$$

$$= \arg \min_{\lambda_k, \alpha_{k,i}, i \in [K]} \mathbb{E}[\|\mathbf{X}_k \tilde{\mathbf{w}}_k - (\mathbf{X}_k \mathbf{w}_k + \mathbf{z})\|_2^2 | \hat{\mathbf{w}}_k, \bar{\theta}_{\setminus k}] \quad (47)$$

$$= \arg \min_{\lambda_k, \alpha_{k,i}, i \in [K]} \mathbb{E}[\|\mathbf{X}_k(\tilde{\mathbf{w}}_k - \mathbf{w}_k)\|_2^2 | \hat{\mathbf{w}}_k, \bar{\theta}_{\setminus k}] \quad (48)$$

$$= \arg \min_{\lambda_k, \alpha_{k,i}, i \in [K]} \mathbb{E}[\|\tilde{\mathbf{w}}_k - \mathbf{w}_k\|_2^2 | \hat{\mathbf{w}}_k, \bar{\theta}_{\setminus k}] \quad (49)$$

then taking (44) and (45) into (49) we have that

$$\lambda_k^* = \sigma^2/v_k^2 \nu \quad (50)$$

$$\alpha_{k,i}^* = \frac{B_k}{\sigma^2 + \beta v_i^2} \quad (51)$$

where $B_k = \frac{A_k(\sigma^2 + \beta v_k^2)}{\sigma^2 + A_k \beta v_k^2}$.

C Further discussion on Theorem 4.2

Theorem 4.2 presents insights on how to set the weights $\{\alpha_{k,i}\}_{i \in [K]}$ and regularization weight λ_k^* for each client $k \in [K]$ from (1) to improve generalization with PERFED-CKT. While in the main paper we discussed the implications of the optimal $\{\alpha_{k,i}^*\}_{i \in [K]}$ in (16) and the motivation for clustering, here we continue the discussion in regards to the optimal $\{\lambda_k^*\}_{k \in [K]}$, i.e., the optimal regularization weight. Recapping the linear regression setup from Section 4, we have θ uniformly distributed on \mathbb{R}^d , and each device $k \in [K]$ has its data distributed with parameters $\mathbf{w}_k = \theta + \zeta_k$ where $\zeta_k \sim \mathcal{N}(0, v_k^2 \mathbf{I}_d)$ and \mathbf{I}_d is the $d \times d$ identity matrix and v_k is unique to the client's task.

Suppose we have $\mathbf{y}_k = \mathbf{X}_k \mathbf{w}_k + \mathbf{z}$, $k \in [K]$ where $\mathbf{y}_k \in \mathbb{R}^n$, $\mathbf{X}_k \in \mathbb{R}^{n \times d}$, and $\mathbf{z} \in \mathbb{R}^n$ such that $\mathbf{z} \sim \mathcal{N}(0, \sigma^2 \mathbf{I}_d)$.

With PERFED-CKT, the optimal regularization weight is equal to $\lambda_k^* = \sigma^2/v_k^2\nu$ as shown in Theorem 4.2, where σ^2 and ν are constant across clients. This shows that clients with large v_k can improve its generalization performance by having a smaller regularization weight. Intuitively, clients that have larger v_k have a higher chance to have larger discrepancy in data distribution from other clients, and therefore having a smaller λ_k can prevent from assimilating irrelevant knowledge from the other clients. Similarly, the opposite also holds where clients with smaller v_k have a higher optimal λ_k^* . This result gives insight into how to set the regularization weight dependent on the client's data discrepancy to other clients. Although in our experiments we use identical λ_k for $k \in [K]$, interesting future directions include varying λ_k of across clients dependent on their data and training progress.

D Generalization Bound for Ensemble Models in Personalization

As defined in Section 3, we have the true data distribution of client k defined as \mathcal{D}_k , and the empirical data distribution associated with the client's training dataset defined as $\widehat{\mathcal{D}}_k$. For a multi-class classification problem with a finite set of classes, we have that the data's domain is defined by the input space $\mathbf{x} \in \mathcal{X}$ and the output space $y \in \mathcal{Y}$. For the generalization bound analysis we consider hypotheses that maps $h : \mathcal{X} \rightarrow \mathcal{Y}$, and \mathcal{H} is defined as the hypotheses space such that $h \in \mathcal{H}$. The loss function $l(h(\mathbf{x}), y)$ measures the classification performance of h for a single data point (\mathbf{x}, y) and we define the expected loss over all data points that follow distribution \mathcal{D} as $\mathcal{L}_{\mathcal{D}}(h) = \mathbb{E}_{(\mathbf{x}, y) \sim \mathcal{D}}[l(h(\mathbf{x}), y)]$. We assume that $\mathcal{L}(\cdot)$ is convex, and is in the range $[0, 1]$. We define the minimizer of the expected loss over the data that follows the distribution \mathcal{D}_k and $\widehat{\mathcal{D}}_k$ as each $h_k = \arg \min_h \mathcal{L}_{\mathcal{D}_k}(h)$ and $\widehat{h}_k = \arg \min_h \mathcal{L}_{\widehat{\mathcal{D}}_k}(h)$. Note that for sufficiently large training dataset, we will have $h_k \simeq \widehat{h}_k$.

Our goal is to show the generalization bound for client k such that $\mathcal{L}_{\mathcal{D}_k}\left(\sum_{i=1}^K \alpha_{k,i} h_{\widehat{\mathcal{D}}_i}\right)$, where $h_{\widehat{\mathcal{D}}_i}$ represents the hypothesis trained from client i 's training dataset and $\alpha_{k,i}$ represents the weight for the hypothesis of client i for client k . For client $i \in [K]$, $h_{\widehat{\mathcal{D}}_i}$ will be the optimal hypothesis with respect to the training dataset for each client participating in FL, and the generalization bound for $\mathcal{L}_{\mathcal{D}_k}\left(\sum_{i=1}^K \alpha_{k,i} h_{\widehat{\mathcal{D}}_i}\right)$ will show how the weighted average of different hypothesis from the other clients with respect to $\alpha_{k,i}$, $i \in [K]$ helps the generalization of an individual client k with respect to its true data distribution. Before presenting the generalization bound, we present several useful lemmas.

Lemma D.1 (Domain adaptation [55]). *With two true distributions \mathcal{D}_A and \mathcal{D}_B , for $\forall \delta \in (0, 1)$ and hypothesis $\forall h \in \mathcal{H}$, with probability at least $1 - \delta$ over the choice of samples, there exists:*

$$\mathcal{L}_{\mathcal{D}_A}(h) \leq \mathcal{L}_{\mathcal{D}_B}(h) + \frac{1}{2}d(\mathcal{D}_A, \mathcal{D}_B) + \nu \quad (52)$$

where $d(\mathcal{D}_A, \mathcal{D}_B)$ measures the distribution discrepancy between two distributions [55] and $\nu = \inf_h \mathcal{L}_{\mathcal{D}_A}(h) + \mathcal{L}_{\mathcal{D}_B}(h)$.

Lemma D.2 (Generalization with limited training samples). *For $\forall k \in [K]$, with probability at least $1 - \delta$ over the choice of samples, there exists:*

$$\mathcal{L}_{\mathcal{D}_k}(h_{\widehat{\mathcal{D}}_k}) \leq \mathcal{L}_{\widehat{\mathcal{D}}_k}(h_{\widehat{\mathcal{D}}_k}) + \sqrt{\frac{\log 2/\delta}{2m_k}} \quad (53)$$

where m_k is the number of training samples of client k . This lemma shows that for small number of training samples, i.e., small m_k , the generalization error increases due to the discrepancy between \mathcal{D}_k and $\widehat{\mathcal{D}}_k$.

Proof. We seek to bound the gap between $\mathcal{L}_{\mathcal{D}_k}(h_{\widehat{\mathcal{D}}_k})$ and $\mathcal{L}_{\widehat{\mathcal{D}}_k}(h_{\widehat{\mathcal{D}}_k})$. Observe that $\mathcal{L}_{\mathcal{D}_k}(h_{\widehat{\mathcal{D}}_k}) = \mathbb{E}[\mathcal{L}_{\widehat{\mathcal{D}}_k}(h_{\widehat{\mathcal{D}}_k})]$, where the expectation is taken over the randomness in the sample draw that generates $\widehat{\mathcal{D}}_k$, and that $\mathcal{L}_{\widehat{\mathcal{D}}_k}(h_{\widehat{\mathcal{D}}_k})$ is an empirical mean over losses $l(h(x), y)$ that lie within $[0, 1]$. Since we

are simply bounding the difference between a sample average of bounded random variables and its expected value, we can directly apply Hoeffding's inequality to obtain

$$\mathbb{P} \left[\mathcal{L}_{\hat{\mathcal{D}}_k}(h_{\hat{\mathcal{D}}_k}) - \mathcal{L}_{\mathcal{D}_k}(h_{\hat{\mathcal{D}}_k}) \geq \epsilon \right] \leq 2e^{-2m\epsilon^2}. \quad (54)$$

Setting the right hand side to δ and rearranging gives the desired bound with probability at least $1 - \delta$ over the choice of samples:

$$\mathcal{L}_{\mathcal{D}_k}(h_{\hat{\mathcal{D}}_k}) \leq \mathcal{L}_{\hat{\mathcal{D}}_k}(h_{\hat{\mathcal{D}}_k}) + \sqrt{\frac{\log 2/\delta}{2m_k}}.$$

□

We now present the generalization bound for $\mathcal{L}_{\mathcal{D}_k} \left(\sum_{i=1}^K \alpha_{k,i} h_{\hat{\mathcal{D}}_i} \right)$ as follows:

$$\mathcal{L}_{\mathcal{D}_k} \left(\sum_{i=1}^K \alpha_{k,i} h_{\hat{\mathcal{D}}_i} \right) \stackrel{(c)}{\leq} \sum_{i=1}^K \alpha_{k,i} \mathcal{L}_{\mathcal{D}_k}(h_{\hat{\mathcal{D}}_i}) \stackrel{(d)}{\leq} \sum_{i=1}^K \alpha_{k,i} [\mathcal{L}_{\mathcal{D}_i}(h_{\hat{\mathcal{D}}_i}) + \frac{1}{2} d(\mathcal{D}_i, \mathcal{D}_k) + \nu_i] \quad (55)$$

where $\nu_i = \inf_h \mathcal{L}_{\mathcal{D}_i}(h) + \mathcal{L}_{\mathcal{D}_k}(h)$, (c) is due to the convexity of \mathcal{L} , and (d) is due to lemma D.1. We can further bound (55) using lemma D.2 as

$$\begin{aligned} \mathcal{L}_{\mathcal{D}_k} \left(\sum_{i=1}^K \alpha_{k,i} h_{\hat{\mathcal{D}}_i} \right) &\leq \sum_{i=1}^K \alpha_{k,i} \mathcal{L}_{\hat{\mathcal{D}}_i}(h_{\hat{\mathcal{D}}_i}) + \sum_{i=1}^K \alpha_{k,i} \sqrt{\frac{\log 2/\delta}{2m_k}} + \frac{1}{2} \sum_{i=1}^K \alpha_{k,i} d(\mathcal{D}_i, \mathcal{D}_k) + \sum_{i=1}^K \alpha_{k,i} \nu_i \\ &= \sum_{i=1}^K \alpha_{k,i} \mathcal{L}_{\hat{\mathcal{D}}_i}(h_{\hat{\mathcal{D}}_i}) + \sqrt{\log \delta^{-1}} \sum_{i=1}^K \frac{\alpha_{k,i}}{\sqrt{m_k}} + \frac{1}{2} \sum_{i=1}^K \alpha_{k,i} d(\mathcal{D}_i, \mathcal{D}_k) + \sum_{i=1}^K \alpha_{k,i} \nu_i \end{aligned} \quad (56)$$

From (57), with $\mathcal{L}_{\hat{\mathcal{D}}_i}(h_{\hat{\mathcal{D}}_i})$ in general being small for $\forall i \in [K]$ as it is the minimum loss, and m_i being similar to other $m_{i'}, i' \in [K]$, the only way to minimize the generalization error of $\mathcal{L}_{\mathcal{D}_k} \left(\sum_{i=1}^K \alpha_{k,i} h_{\hat{\mathcal{D}}_i} \right)$ is to set the weights $\alpha_{k,i}$ so that the third term $\frac{1}{2} \sum_{i=1}^K \alpha_{k,i} d(\mathcal{D}_i, \mathcal{D}_k)$ is minimized. Note that it is difficult to know the value of ν_i , making it impractical to minimize the fourth term in practice. This generalization results strengthens our motivation to use to find the weights $\alpha_{k,i}, i \in [K]$ that minimizes $\frac{1}{|\mathcal{P}|} \sum_{\mathbf{x} \in \mathcal{P}} \|\sum_{i=1}^K \alpha_{k,i} s_i(\mathbf{w}_i, \mathbf{x}) - s(\mathbf{w}_k, \mathbf{x})\|_2^2$ in regards to the objective function we have in (1).

E Details of Experimental Setup

Codes for the results in the paper are presented in the supplementary material.

Description for Toy Example - Figure 1

For Figure 1, we design a linear regression problem where the true local model for each client is generated as $\mathbf{w}_i = \theta + \zeta_i, i \in [3]$ where $\theta \in \mathbb{R}^{2 \times 1}$ is a non-informative prior which elements are uniformly distributed $\mathcal{U}(-10, 10)$ and the elements of ζ_i follows the normal distribution $\mathcal{N}(0, \sigma_i)$, $\sigma_1 = 2, \sigma_2 = 5, \sigma_3 = 200$. The discrepancy across the variance denotes the data-heterogeneity across the clients. The range for \mathbf{x} is $[-10, 10]$ for all elements. We assume all clients have identical dataset size. For implementing PERFED-CKT for the toy example, we set the public data range as identical to the input data range, and set $\lambda = 50$. For KT w/o clustering, the co-distillation term uses a simple average of all the logits from the clients for regularizing while for KT with clustering the weights are set so that clients with similar true local models have higher weights for each other. This setting is also consistent with the generalization analysis presented in Section 4. The code for the linear regression toy example is presented in the supplementary material.

Description for CIFAR10 Experiments.

Data Partitioning. We experiment with three different seeds for the randomness in the dataset partition across clients and present the averaged results across the seeds with the standard deviation. The partitioning of each individual client’s data to training/validation/test dataset is done as follows: after partitioning the entire dataset by the Dirichlet distribution $\text{Dir}_K(\alpha)$ with $\alpha = 0.01$ across clients, we partition each client dataset by a $\{0.1, 0.3, 0.4\}/0.1/0.5$ ratio where the ratio for the training dataset is chosen by random from $\{0.1, 0.3, 0.4\}$ for each client. Such partitioning simulates a more realistic FL setting where individual clients may not have sufficient labeled data samples for training that represents the test dataset’s distribution. For all experiments we run 500 communication rounds which we have observed allows convergence for all experiments.

Local Training and Hyperparameters. For the local-training hyperparameters, we do a grid search over the learning rate: $\eta \in \{0.1, 0.05, 0.01, 0.005, 0.001\}$, batchsize: $b \in \{32, 64, 128\}$, and local iterations: $\tau \in \{10, 30, 50\}$ to find the hyper-parameters with the highest test accuracy for each benchmark. For all benchmarks we use the best hyper-parameter for each benchmark after doing a grid search over feasible parameters referring to their source codes that are open-sourced. For the knowledge distillation server-side hyperparameters, we do a grid search over the public batch size: $b' \in \{32, 64, 128\}$, regularization weight $\lambda \in \{0.05, 0.1, 0.5, 1, 2, 4\}$ to find the best working hyperparameters. The best hyperparameters for PERFED-CKT we use is $\eta = 0.001, b = 64, \tau = 50, b' = 128, \lambda = 2$.

Model Setup. For the model configuration, for the CNN we have a self-defined convolutional neural network with 2 convolutional layers with max pooling and 4 hidden fully connected linear layers of units [120, 100, 84, 50]. The input is the flattened convolution output and the output is consisted of 10 units each of one of the 0-9 labels. For the VGG, we use the open-sourced VGG net from Pytorch with torchvision ver.0.4.1 presented in Pytorch without pretrained as False and batchnorm as True.

Platform. All experiments are conducted with clusters equipped with one NVIDIA TitanX GPU. The number of clusters we use vary by C , the fraction of clients we select. The machines communicate amongst each other through Ethernet to transfer the model parameters and information necessary for client selection. Each machine is regarded as one client in the federated learning setting. The algorithms are implemented by PyTorch.