
One for One, or All for All: Equilibria and Optimality of Collaboration in Federated Learning

Avrim Blum¹ Nika Haghtalab² Richard Lanus Phillips³ Han Shao¹

Abstract

In recent years, federated learning has been embraced as an approach for bringing about collaboration across large populations of learning agents. However, little is known about how collaboration protocols should take agents' incentives into account when allocating individual resources for communal learning in order to maintain such collaborations. Inspired by game theoretic notions, this paper introduces a framework for incentive-aware learning and data sharing in federated learning. Our stable and envy-free equilibria capture notions of collaboration in the presence of agents interested in meeting their learning objectives while keeping their own sample collection burden low. For example, in an envy-free equilibrium, no agent would wish to swap their sampling burden with any other agent and in a stable equilibrium, no agent would wish to unilaterally reduce their sampling burden.

In addition to formalizing this framework, our contributions include characterizing the structural properties of such equilibria, proving when they exist, and showing how they can be computed. Furthermore, we compare the sample complexity of incentive-aware collaboration with that of optimal collaboration when one ignores agents' incentives.

1. Introduction

In recent years, federated learning has been embraced as an approach for enabling large numbers of learning agents to collaboratively accomplish their goals using collectively fewer resources, such as smaller data sets. Indeed, collaborative protocols are starting to be used across networks of hos-

pitals (Wen et al., 2019; Powell, 2019) and devices (McMahan & Ramage, 2017) and are behind important breakthroughs such as understanding the biological mechanisms underlying schizophrenia in a large scale collaboration of more than 100 agencies (Bergen & Petryshen, 2012).

This promise of creating large scale impact from mass participation has led to federated learning receiving substantial interest in the machine learning research community, and has resulted in faster and more communication-efficient collaborative systems. But, what will ultimately decide the success and impact of collaborative federated learning is the ability to recruit and retain large numbers of learning agents — a feat that requires collaborative algorithms to

help agents accomplish their learning objectives while “equitably” spreading the data contribution responsibilities among agents who want a lower sample collection burden.

This is to avoid the following inequitable circumstances that may otherwise arise in collaborative learning. First, when part of an agent's data is exclusively used to accomplish another agent's learning goals; for example, if an agent's learning task can be accomplished even when she (unilaterally) lowers her data contribution. Second, when an agent envies another agent; for example, if an agent's learning goal can be accomplished even when she swaps her contribution burden with another agent who has a lower burden.

In this paper, we introduce the first comprehensive game theoretic framework for collaborative federated learning in the presence of agents who are interested in accomplishing their learning objectives while keeping their individual sample collection burden low. Our framework introduces two notions of equilibria that avoid the aforementioned inequities. First, analogous to the concept of Nash equilibrium (Nash, 1951), our *stable equilibrium* requires that no agent could unilaterally reduce her data contribution responsibility and still accomplish her learning objective. Second, inspired by the concept of envy-free allocations (Foley, 1967; Varian, 1974), our *envy-free equilibrium* requires that no agent could swap her data contribution with an agent with lower contribution level and still accomplish her learning objective. In addition to capturing what is deemed as an “equitable” collaboration to agents, using stable and envy-free equilibria

*Equal contribution ¹Toyota Technological Institute ²University of California, Berkeley ³Cornell University. Correspondence to: <nika@berkeley.edu>.

is essential for keeping learning participants fully engaged in ongoing collaborations.

Our framework is especially useful for analyzing how the sample complexity of federated learning may be affected by the agents’ desire to keep their individual sample complexities low. To demonstrate this, we work with three classes as running examples of agent learning objectives: random discovery (aka linear) utilities, random coverage utilities, and general PAC learning utilities. Our results answer the following qualitative and quantitative questions:

Existence of Equilibria. In Section 3, we show that the existence of a stable equilibrium depends on whether agents’ learning objectives are “well-behaved”. In particular, we see that in the PAC learning setting, there may not exist a stable equilibrium, but under mild assumptions, a stable equilibrium exists in the random discovery and random coverage settings. On the other hand, an envy-free equilibrium with equal agent contribution trivially exists.

Sample Complexity of Equilibria. In Section 4, we show that even for well-behaved learning objectives, such as random discovery and random coverage examples, there is a large gap between the socially optimal sample complexity and the optimal sample complexity achieved by any equilibrium. In particular, we show that there is a factor $\Omega(\sqrt{k})$ gap between the socially optimal sample complexity and that of optimal stable or envy-free equilibria for k agents.

Algorithmic and Structural Properties. The main result of Section 5 shows that in the random discovery setting, in every optimal stable equilibrium there is a core-set of agents for whom *the equilibrium happens to also be socially optimal*, and agents who do not belong to this set make 0 contribution in the equilibrium. This result allows us to characterize classes of problems where the optimal stable equilibria are also socially optimal. We further show that in some cases, linear or convex programs can be used to compute socially optimal or optimal stable equilibria.

Empirical Analysis. We show that some commonly used federated algorithms produce solutions that are very far from being an equilibrium. We show that the Federated-Averaging (FedAvg) algorithm of McMahan et al. (2017) lead to solutions where a large number of agents would rather reduce their contribution to as little as 25% to 1%. We also work with the Multiplicative Weight Update style algorithm (MW-FED) of Blum et al. (2017) and show that this algorithm produces allocations that are closer to being an equilibrium, but more work is needed for designing algorithms that further close this gap.

1.1. Related Work.

Federated learning and the model aggregation algorithm FedAvg were proposed by McMahan et al. (2017). The

collaborative learning framework of Blum et al. (2017) studied heterogeneous learning objectives in federated learning and quantified how sample complexity improves with more collaboration. However, except for a few recent works discussed below, agents’ incentives have not been addressed in these frameworks.

Lyu et al. (2020); Yu et al. (2020); Zhang et al. (2020) proposed several fairness metrics for federated learning that reward high-contributing agents with higher payoffs, however, they do not consider strategicness of agents and the need for equilibrium. Li et al. (2019) empirically studied a different fairness notion of uniform accuracy across devices without discussing data contribution, while our work allows for different accuracy levels so long as every learner’s objective is accomplished and focuses data contribution. Sim et al. (2020) proposed a reward scheme based on the Shapley value to provide incentive for collaboration when each agent’s sampling burden is fixed. Recently, Donahue & Kleinberg (2021) studied individual rationality in federated learning when global models may be worse than an agent’s local model and used concepts from hedonic game theory to discuss coalition formation. Other works have discussed issues of free-riders and reputation (Lin et al., 2019; Kang et al., 2019) as well as markets and credit sharing in machine learning (Ghorbani & Zou, 2019; Agarwal et al., 2019; Balkanski et al., 2017; Jia et al., 2019).

2. Problem Formulation

Let us start this section with a motivating example before introducing our general model in Section 2.1.

Consider the collaborative learning problem with k agents with distributions $\mathcal{D}_1, \dots, \mathcal{D}_k$. For each agent $i \in [k]$, her goal is to satisfy the constraint of low expected error, i.e.,

$$\mathbb{E}_{\{S_j \sim \mathcal{D}_j^{m_j}\}_{j \in [k]}} [\text{err}_{\mathcal{D}_i}(h_S)] \leq \varepsilon, \quad (1)$$

for some $\varepsilon > 0$, where each agent j takes $m_j \geq 0$ random samples $S_j \sim \mathcal{D}_j^{m_j}$ and h_S is a prediction rule based on $S = \cup_{j \in [k]} S_j$. Then the sample complexity of federated learning is the optimal allocation (m_1, \dots, m_k) that minimizes the total number of samples conditioned on satisfying every agent’s accuracy constraint, that is,

$$\begin{aligned} \min \quad & \sum_{i=1}^k m_i \\ \text{s. t.} \quad & \mathbb{E}_{\{S_j \sim \mathcal{D}_j^{m_j}\}_{j \in [k]}} [\text{err}_{\mathcal{D}_i}(h_S)] \leq \varepsilon, \forall i \in [k]. \end{aligned} \quad (2)$$

It is not surprising that **optimizing Equation (2) requires collectively fewer samples** than the total number of samples agents need to individually solve Equation (1)¹, **but the optimal solution to Equation (2) may unfairly require one**

¹Blum et al. (2017) upper and lower bound this improvement.

or more agents to contribute larger sample sets than could reasonably be expected from them. Our notion of a *stable equilibrium* requires that no agent j , conditioned on keeping her constraint satisfied, can unilaterally reduce m_j . On the other hand, our *envy-free equilibrium* requires that no agent j , conditioned on keeping her constraint satisfied, can swap m_j with another agent's contribution $m_i < m_j$. Taking stability and envy-freeness as constraints, we ask whether such notions of equilibria always exist and whether stable and envy-free sample complexities are significantly worse than the optimal solution to Equation (2).

2.1. The General Framework

In this paper, we study this problem in a more general setting where there are k agents and all agents collaboratively select a strategy $\theta = (\theta_1, \dots, \theta_k)$ from a strategy space $\Theta \subseteq \mathbb{R}_+^k$. Each agent i selects a number θ_i as her *contribution level*, e.g., the number of samples. We define $u_i : \Theta \mapsto \mathbb{R}$ as the utility function for each agent i and her goal is to achieve

$$u_i(\theta) \geq \mu_i$$

for some μ_i . This utility function is a generalization of the expected accuracy in our motivating example and $\mu_i = 1 - \varepsilon$ is the minimum accuracy required by the agent.

For any $\theta \in \mathbb{R}^k$, $x \in \mathbb{R}$, let $(x, \theta_{-i}) \in \mathbb{R}^k$ denote the vector with the i -th entry being x and the j -th entry being θ_j for $j \neq i$. Without loss of generality, we assume that every agent can satisfy her constraint individually, i.e., $\forall i \in [k]$, $\exists \vartheta_i \in \mathbb{R}_+^k$ such that $u_i(\vartheta_i, \mathbf{0}_{-i}) \geq \mu_i$ and u_i is non-decreasing with θ_j for any j .

We say that θ is *feasible* if $u_i(\theta) \geq \mu_i$ for all $i \in [k]$. We define the socially optimal solution analogously to Equation (2) as the optimal feasible solution that does not consider agents' incentives.

Definition 1 (Optimal solution (OPT)). θ^{opt} is a socially optimal solution in Θ if it is the optimal solution to the following program

$$\begin{aligned} & \min_{\theta \in \Theta} \mathbf{1}^\top \theta \\ & \text{s. t. } u_i(\theta) \geq \mu_i, \forall i \in [k]. \end{aligned} \quad (3)$$

A stable equilibrium is a feasible solution where no player has incentive to unilaterally decrease her strategy.

Definition 2 (Stable equilibrium (EQ)). A feasible solution θ^{eq} is a stable equilibrium over Θ if for any $i \in [k]$, there is no $(\theta'_i, \theta_{-i}^{\text{eq}}) \in \Theta$ such that $\theta'_i < \theta_i^{\text{eq}}$ and $u_i(\theta'_i, \theta_{-i}^{\text{eq}}) \geq \mu_i$.

An *envy-free equilibrium* is a feasible solution where no agent has an incentive to swap their sampling load with another agent. For any θ , let $\theta^{(i,j)}$ denote the θ when the i -th and the j -th entries are swapped, i.e., $\theta_i^{(i,j)} = \theta_j$, $\theta_j^{(i,j)} = \theta_i$ and $\theta_l^{(i,j)} = \theta_l$ for $l \neq i, j$.

Definition 3 (Envy-free equilibrium (EF)). A feasible solution θ^{ef} is envy-free if for any $i \in [k]$, there is no $\theta^{\text{ef}(i,j)} \in \Theta$ such that $\theta_j^{\text{ef}} < \theta_i^{\text{ef}}$ and $u_i(\theta^{\text{ef}(i,j)}) \geq \mu_i$.

We call an equilibrium θ optimal if it is an equilibrium with minimal resources, i.e., minimizes $\mathbf{1}^\top \theta$.

We use the game theoretic quantities known as the *Price of Stability* (Anshelevich et al., 2008) and the *Price of Fairness* (Caragiannis et al., 2012) to quantify the impact of equilibria on the efficiency of collaboration.

Definition 4 (Price of Stability). *Price of Stability (PoS)* is defined as the ratio of the value of the optimal stable equilibrium to that of the socially optimal solution. That is, letting $\Theta^{\text{eq}} \subseteq \Theta$ be the set of all stable equilibria, $\text{PoS} = \min_{\theta \in \Theta^{\text{eq}}} \mathbf{1}^\top \theta / \mathbf{1}^\top \theta^{\text{opt}}$.

Definition 5 (Price of Fairness). *Price of Fairness (PoF)* is defined as the ratio of the value of the optimal envy-free equilibrium to that of the socially optimal solution. That is, letting $\Theta^{\text{ef}} \subseteq \Theta$ be the set of all envy-free equilibria, $\text{PoF} = \min_{\theta \in \Theta^{\text{ef}}} \mathbf{1}^\top \theta / \mathbf{1}^\top \theta^{\text{opt}}$.

2.2. Canonical Examples and Settings

We use the following three canonical settings as running examples throughout the paper.

Random Discovery aka Linear Utilities. We start with a setting where any agent's utility is a linear combination of the efforts other agents put into solving the problem. As a general setting, we let $\mathbf{u}(\theta) = W\theta$ for matrix $W \in [0, 1]^{k \times k}$, where W_{ij} denotes how the effort of agent j affects the utility of agent i . We commonly assume that W is a symmetric PSD matrix with an all one diagonal.

As an example, consider a setting where each agent i has a distribution \mathbf{q}_i over the instance space \mathcal{X} with $|\mathcal{X}| = n$, and where the agent i receives a reward proportional to the density of q_{ix} every time an instance x is realized (or discovered) by any agent's sampling effort. Formally, the utility of agent i in strategy θ is her expected reward:

$$u_i(\theta) = \mathbf{q}_i Q^\top \theta,$$

where $Q = [q_{ix}] \in \mathbb{R}_+^{k \times n}$ denote the matrix with the (i, x) -th entry being q_{ix} , we have that $\mathbf{u}(\theta) = QQ^\top \theta$ is a linear function. Note that in this case, $W = QQ^\top$ is indeed a symmetric PSD matrix.

Random Coverage. While in our previous example an agent draws utility *everytime* an instance x is discovered, in many classification settings, the utility of an agent is determined by whether x has been observed at all (and not

the number of its observations).² This gives rise to the non-linear utilities we define below.

Consider a simple binary classification setting where the label of each point is uniformly labeled positive or negative independently of all others. More specifically, assume that the domain \mathcal{X} is labeled according to a target function f^* that is chosen uniformly at random from $\{\pm 1\}^{\mathcal{X}}$. Each agent i has a distribution \mathbf{q}_i over the instance space \mathcal{X} . Note that given any set of observed points $S = \{x_1, \dots, x_m\} \subseteq \mathcal{X}$ and their corresponding revealed labels $f^*(x)$ for $x \in S$. The optimal classifier h_S classifies each $x \in S$ correctly as $f^*(x)$ and misclassifies each $x \notin S$ with probability $1/2$. Let $u_i(\boldsymbol{\theta})$ be the expected accuracy of the optimal classifier where agent i took an integral value θ_i number of samples, i.e.,

$$u_i(\boldsymbol{\theta}) = 1 - \frac{1}{2} \sum_{x \in \mathcal{X}} q_{ix} \prod_{j=1}^k (1 - q_{jx})^{\theta_j}.$$

Throughout the paper, we consider the general random coverage setting introduced here and its simpler variants where all agents' distributions are uniform over equally-sized sets.

As opposed to the linear utilities, non-integral values of θ_i (as mean of a distribution over integers) are not as easily interpretable. Indeed, the same θ_i may refer to distributions with different expected utilities. Here we consider one natural interpretation of a real-valued θ_i : randomized rounding over $\lfloor \theta_i \rfloor$ and $\lceil \theta_i \rceil$ with mean of θ_i . See Appendix A for more information.

General PAC Learning. Now we consider a general learning setting, where the labels of points are not necessarily independent. In this case, the optimal classifier can improve its accuracy on unobserved points based on those points' dependence on observed points. For example, consider a scenario where an input space \mathcal{X} where $|\mathcal{X}| = 2$ and a hypothesis class that always labels points in \mathcal{X} either both positive or negative. Then, if only one point is observed, the classifier will classify the unobserved point the same as the label of the observed one.

Generally, given input space \mathcal{X} and agent i 's distribution \mathcal{D}_i over \mathcal{X} , we let utility function $u_i(\boldsymbol{\theta})$ be the expected accuracy of an optimal predictor h_S given training data set $S = \cup_{j \in [k]} S_j$ when agent i takes an integral value θ_i number of samples,

$$u_i(\boldsymbol{\theta}) = 1 - \mathbb{E}_{\{S_j \sim \mathcal{D}_j^{\theta_j}\}_{j \in [k]}} [\text{err}_{\mathcal{D}_i}(h_S)].$$

Similar to the random coverage settings, we interpret real values θ_i as the appropriate distribution over $\lfloor \theta_i \rfloor$ and $\lceil \theta_i \rceil$ whose mean is θ_i .

²Note that the two cases approximate one another if the number of samples to be taken is much smaller than the size of the domain i.e., $(1 - p_i)^m \approx 1 - mp_i$.

3. Existence of Equilibria

In this section, we discuss the existence of stable and envy-free equilibria in collaborative federated learning. Clearly, any solution with equal allocation among all agents is an envy-free allocation. That is, any feasible allocation $\boldsymbol{\theta}$ can be converted to an envy-free allocation $\boldsymbol{\theta}^{\text{ef}}$ by letting $\forall i \in [k], \theta_i^{\text{ef}} = \max_j \theta_j$.

Theorem 1. *An envy-free solution always exists in a feasible collaborative learning problem.*

In the aforementioned envy-free solution $\boldsymbol{\theta}^{\text{ef}}$, however, all agents (except for those with the maximum allocation) could unilaterally reduce their allocations while meeting their constraints, so $\boldsymbol{\theta}^{\text{ef}}$ is not an equilibrium. Indeed, in the remainder of this section we show that existence of an equilibrium in collaborative learning depends on the precise setting of the problem. In particular, we show that an equilibrium solution exists when unilateral deviations in an agent's contribution has a bounded impact on the utility of any agent. On the other hand, an equilibrium solution may not exist if infinitesimally small changes to an agent's contribution has an outsized effect on other agents' utilities (or if an agent's strategy space is not even continuous).

We will formalize this in the next definition. Broadly, this definition states that an agent's utility increases at a positive (and bounded away from zero) rate when the agent unilaterally increases her contribution. Moreover, an agent's utility does not increase at an infinite rate. In other words, it is bounded above by a constant when other agents unilaterally increase their contributions.

Definition 6 (Well-behaved Utility Functions). *We say that a set of utility functions $\{u_i : \Theta \rightarrow \mathbb{R} \mid i \in [k]\}$ is well-behaved over $\times_{i=1}^k [0, C_i] \subseteq \Theta$ for some C_i 's, if and for each agent $i \in [k]$ there are constants $c_1^i \geq 0$ and $c_2^i > 0$ such that for any $\boldsymbol{\theta} \in \times_{i=1}^k [0, C_i]$,*

1. $\partial u_i(\boldsymbol{\theta}) / \partial \theta_i \geq c_2^i$; and
2. for all $j \in [k]$ and $j \neq i$, $0 \leq \partial u_i(\boldsymbol{\theta}) / \partial \theta_j \leq c_1^i$.

We emphasize that the utility functions that correspond to many natural learning settings and domains, such as in the linear case and random coverage, are well-behaved. That being said, it is also not hard to construct natural learning settings where the utility functions are not well-behaved, e.g., when an agent is restricted to taking an integral number of samples and therefore its utility is not continuous. In the remainder of this section, we prove that, when agent utilities are well-behaved, an equilibrium exists.

Theorem 2. *For any collaborative learning problem with utility functions u_i s and μ_i s, let ϑ_i represent the individually satisfying strategy such that $u_i(\vartheta_i, \mathbf{0}_{-i}) \geq \mu_i$. If u_i s are*

well-behaved over $\times_{i=1}^k [0, \vartheta_i]$, then there exists an equilibrium.

We complement this positive result by constructing a natural learning setting that corresponds to ill-behaved utility functions and show that this problem has no equilibrium.

Theorem 3. *There is a feasible collaborative learning problem in the general PAC learning setting that does not have an equilibrium.*

3.1. Are Canonical Examples Well-behaved?

Recalling the three canonical examples introduced in Section 2.2, here we discuss whether they are well-behaved or not. It is not hard to see that linear utilities are well-behaved as u_i increases at a constant rate W_{ij} when agent j increases her strategy unilaterally, $W_{ii} = 1$, and $W_{ij} \leq 1$.

In the random coverage case, the utilities are well-behaved over $\times_{i=1}^k [0, \vartheta_i]$ as long as $u_i(\vartheta_i + 1, \vartheta_{-i}) - u_i(\vartheta)$ is bounded away from 0. For example, this is the case when $\mu \in [\frac{1}{2}, C]^k$ for $C < 1$ that is bounded away from 1.

At a high level, the smallest impact that an additional sample by agent i has on u_i is when $\theta \rightarrow \vartheta$. This impact is at least $u_i(\vartheta_i + 1, \vartheta_{-i}) - u_i(\vartheta) > 0$. On the other hand, $\partial u_i(\theta)/\partial \theta_j$ is bounded above, because the marginal impact of any one sample on u_i is largest when no agent has yet taken a sample. Therefore, this impact is at least $u_i(1, \mathbf{0}_{-j}) - u_i(\mathbf{0}) = 1/2 \sum_{x \in \mathcal{X}} q_{ix} q_{jx} \leq 1/2$. This shows that under mild assumption the random coverage utilities are well-behaved.

We note that the range of $\times_{i=1}^k [0, C_i]$ and the continuity of Θ plays an important role in determining the behavior. For example, none of these utility functions are well-behaved over the set of integers, since $\partial u_i(\theta)/\partial \theta_j$ is undefined. More detail can be found in Appendix B.

3.2. Proof of Theorem 2

In this section, we prove Theorem 2 and show that an equilibrium exists when utility functions are well-behaved. Our main technical tool is to show that the best-response dynamic has a fixed point. We define a *best-response* function $\mathbf{f} : \times_{i=1}^k [0, \vartheta_i] \mapsto \times_{i=1}^k [0, \vartheta_i]$ that maps any θ to θ' , where θ'_i is the minimum contribution agent i has to make so that $u_i(\theta'_i, \theta_{-i}) \geq \mu_i$. This is formally defined by $\mathbf{f}(\theta) := (f_i(\theta))_{i \in [k]}$, where

$$f_i(\theta) = \arg \min_{x \geq 0} u_i(x, \theta_{-i}) \geq \mu_i.$$

Due to the monotonicity of u_i s and the definition of ϑ_i s, it is easy to show that $f_i(\theta) \leq \vartheta_i$.

Fixed points of function \mathbf{f} , i.e., those θ for which $\mathbf{f}(\theta) = \theta$, refer to the equilibria of the collaborative learning game.

This is because, by definition, $f_i(\theta)$ is the smallest contribution from agent i that can satisfy agent i 's constraint in response to other agents' contributions θ_{-i} . Therefore, when $\theta_i = f_i(\theta)$ for all $i \in [k]$, no agent can unilaterally reduce their contribution and still satisfy their constraint. That is, such θ is an equilibrium. Therefore, to prove Theorem 2, it suffices to show that the best-response function \mathbf{f} has a fixed point.

Lemma 1. *If utilities are well-behaved over $\times_{i=1}^k [0, \vartheta_i]$, the best-response function \mathbf{f} has a fixed point, i.e., $\exists \theta \in \times_{i=1}^k [0, \vartheta_i], \mathbf{f}(\theta) = \theta$.*

We defer the proof of Lemma 1 to Appendix C. At a high level, we show that \mathbf{f} is continuous because, for well-behaved utility functions, a small change in other agents' contributions affects the utility of agent i only by a small amount. Thus, a small adjustment to agent i 's contribution will be sufficient to re-establish her constraint when other agents make infinitesimally small adjustments to their strategies. Then, combining this with the celebrated Brouwer fixed-point theorem proves this lemma.

3.3. Proof of Theorem 3

In this section, we prove Theorem 3 and show that an equilibrium might not exist if the utility functions are not well-behaved. We demonstrate this using a simple example where the utility function corresponds to the accuracy of classifiers in a general PAC learning setting with integral value strategies. We give a more general construction in Appendix D.

We consider the problem in the binary classification setting where one agent's marginal distribution reveals information about the optimal classifier for another agent.

Consider the domain $\mathcal{X} = \{0, \dots, 5\}$ and the label space $\mathcal{Y} = \{0, 1\}$. We consider agents $\{0, 1, 2\}$ with distributions $\mathcal{D}_0, \mathcal{D}_1, \mathcal{D}_2$ over $\mathcal{X} \times \mathcal{Y}$. Let \oplus and \ominus denote addition and subtraction modulo 3.

We give a probabilistic construction for $\mathcal{D}_0, \mathcal{D}_1, \mathcal{D}_2$. Take independent random variables Z_0, Z_1, Z_2 that are each uniform over $\{0, 1\}$. For each $i \in \{0, 1, 2\}$, distribution \mathcal{D}_i is a point distribution over a single instance-label pair $(2i + z_i, z_{i \oplus 1})$. In other words, the marginal distribution of \mathcal{D}_i is equally likely to be the point distribution on $2i$ or $2i + 1$. Moreover, the labels of points in distribution $\mathcal{D}_{i \oplus 1}$ are decided according to the marginal distribution of \mathcal{D}_i : If the marginal distribution of \mathcal{D}_i is a point distribution supported on $2i$ then any point in $\mathcal{D}_{i \oplus 1}$ is labeled 0, and if the marginal distribution of \mathcal{D}_i is a point distribution on $2i + 1$ then any point in $\mathcal{D}_{i \oplus 1}$ is labeled 1.

Consider the optimal classifier conditioned on the event where agent i takes a sample $(2i + z_i, z_{i \oplus 1})$ from \mathcal{D}_i and no other agents takes any samples. This reveals z_i and $z_{i \oplus 1}$.

Therefore, the optimal classifier conditioned on this event achieves an accuracy of 1 for agent i (by classifying $2i$ and $2i + 1$ as $z_{i \ominus 1}$) and agent $i \oplus 1$ (by classifying $2(i \oplus 1)$ and $2(i \oplus 1) + 1$ as z_i). On the other hand, the optimal label for instances owned by agent $i \ominus 1$, is $Z_{i \oplus 1}$. By the independence of random variables Z_0, Z_1 , and Z_2 , we have that $Z_{i \oplus 1}$ is uniformly random over $\{0, 1\}$ even conditioned on z_i and $z_{i \ominus 1}$. Therefore, the optimal classifier has an expected error of $1/2$ for agent $i \ominus 1$. Using a similar analysis, if any two agents each take a single sample from their distributions, the accuracy of the optimal classifier for all agents is 1.

We now formally define the strategy space and utility functions that correspond to this setting. Let $\Theta = \{0, 1\}^3$ to be the set of strategies in which each agent takes zero or one sample. Let $\mu = 1$. Let $u_i(\theta)$ be the expected accuracy of the optimal classifier given the samples taken at random under θ . As a consequence of the above analysis,

$$u_i(\theta) = \begin{cases} 1 & \theta_i = 1 \text{ or } \theta_{i \ominus 1} = 1 \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

Note that any $\theta \in \Theta$ for which $\|\theta\|_1 \geq 2$ is a feasible solution, while no $\|\theta\|_1 \leq 1$ is a feasible solution. Now consider any θ for which $\|\theta\|_1 \geq 2$. Without loss of generality, there must be an agent i such that $\theta_i = \theta_{i \ominus 1} = 1$. Since $\theta_{i \ominus 1} = 1$, we also have that $u_i(0, \theta_{-i}) = 1$. That is agent i can deviate from the strategy and still meet her constraint. Therefore, no feasible solution is a stable equilibrium. This proves Theorem 3.

4. Quantitative Bounds on Price of Stability and Price of Fairness

As shown in Section 3, while an envy-free solution always exists, the existence of stable equilibria depends on the properties of the utility function. In this section, we go beyond existence and give quantitative bounds on the suboptimality of these equilibria notions even when they exist in the presence of (very) well-behaved functions.

Theorem 4. *There is a collaborative learning setting with well-behaved utility functions such that the Price of Stability and Price of Fairness are at least $\Omega(\sqrt{k})$. Moreover, these utilities correspond to two settings: a) a random domain coverage example with uniform distributions over equally sized subsets and b) a linear utility setting with $W_{ii} = 1$ and $W_{ij} \in O(1/\sqrt{k})$ for $j \neq i$.*

We provide an overview of the proof of Theorem 4 here and defer the details of this proof to Appendix E. Our construction for the random coverage and linear utility settings are very similar, here we only discuss the random coverage setting. The crux of our approach is to build a set structure

where one agent, called the core, overlaps with all other agents and no two agent sets intersect outside of the core. We use a relatively small μ_i s so that every agent only needs to observe one of the points in her set. In our construction, the core is the most “efficient” agent in reducing the error of all other agents and optimal collaboration puts a heavy sampling load (of about \sqrt{k}) on the core. Moreover, because the core includes all the points on which two other agents intersect, the core’s constraint is also easily satisfied when any other agent’s constraint is satisfied. This means that in no stable or envy-free equilibrium can the core take more samples than another agent. Therefore, most of the work has to be done by other agents in any equilibrium allocation, which requires a total of k samples. This tradeoff between being both the most “efficient” at sampling to reduce error and having an “easy-to-satisfy constraint” leads to a large Price of Stability and Price of Fairness.

5. Structural and Algorithmic Perspectives

In this section, we take a closer look at the stable equilibria of the two canonical example where they are guaranteed to exist, i.e., the linear utilities and the coverage utilities, and study their structural and computational aspects.

5.1. Algorithms for Linear Utility

Recall that linear utility functions are functions $\mathbf{u}(\theta) = W\theta$ where $W \in [0, 1]^{k \times k}$, where W_{ij} denotes how the efforts of agent j affects the utility of agent i . In this section, we assume that W is a symmetric PSD matrix ³ with an all 1 diagonal.

An immediate consequence of linear utilities is that the optimal collaborative solution can be computed using the following linear program efficiently

$$\begin{aligned} \min \quad & \sum_{i=1}^k \theta_i \\ \text{s. t.} \quad & W\theta \geq \mu \\ & \theta \geq 0. \end{aligned} \tag{LP 1}$$

Interestingly, the set of stable equilibria of linear utilities are also convex and the optimal stable equilibrium can be computed using a convex program. To see this, note that any solution to LP 1 satisfies the constraints $\theta_i(W_i^\top \theta - \mu_i) \geq 0, \forall i \in [k]$, where W_i denotes the i -th column of W . Hence, adding the constraints $\theta_i(W_i^\top \theta - \mu_i) \leq 0, \forall i \in [k]$ to LP 1 will further restrict the solution to be a stable equilibrium where $\theta_i = 0$ or $W_i^\top \theta = \mu_i$. Given that any stable equilibrium meets both of these constraints with tight equality of 0, they can be equivalently represented by the following convex program.

Theorem 5. *The following convex program computes an*

³This matches our motivating use-case defined in Section 2

optimal stable equilibrium of collaborative learning with linear utility functions

$$\begin{aligned} \min \quad & \sum_{i=1}^k \theta_i \\ \text{s. t.} \quad & W\theta \geq \mu \\ & \theta \geq 0 \\ & \theta^\top W\theta - \mu^\top \theta \leq 0, \end{aligned} \quad (\text{CP } 1)$$

where the last inequality is convex when W is PSD.

5.2. Structure of Equilibria for Linear Utility

In this section, we take a closer look at the structural properties of stable and envy-free equilibria and provide a qualitative comparison between them and the optimal solutions. The main result of this section is that in any optimal stable equilibrium, there is a core subset of k agents for which the equilibrium is also a socially optimal collaboration, while all other agents' contributions are fixed at 0.

Theorem 6. *Let θ^{eq} be an optimal stable equilibrium for linear utilities $u_i(\theta) = W_i^\top \theta$ and $\mu_i = \mu$ for $i \in [k]$, where W is a symmetric PSD matrix. Let $I_{\theta^{\text{eq}}} = \{i \mid \theta_i^{\text{eq}} = 0\}$ be the set of non-contributing agents and let \bar{W} and $\bar{\theta}^{\text{eq}}$ be the restriction of W and θ^{eq} to $[k] \setminus I_{\theta^{\text{eq}}}$. Then $\bar{\theta}^{\text{eq}}$ is a socially optimal solution for the set of agents $i \in [k] \setminus I_{\theta^{\text{eq}}}$, i.e., agents with utilities $u_i(\bar{\theta}) = \bar{W}_i^\top \bar{\theta}$ for $i \in [k] \setminus I_{\theta^{\text{eq}}}$.*

Furthermore, let $\tilde{\theta}$ represent the extension of $\bar{\theta}$ by padding 0s at $I_{\theta^{\text{eq}}}$, i.e., $\tilde{\theta}_i = 0$ for $i \in I_{\theta^{\text{eq}}}$ and $\tilde{\theta}_i = \bar{\theta}_i$ for $i \in [k] \setminus I_{\theta^{\text{eq}}}$. For any $\bar{\theta}$ that is a socially optimal solution for agents $[k] \setminus I_{\theta^{\text{eq}}}$, $\tilde{\theta}$ is an optimal stable equilibrium for agents $[k]$.

This theorem implies that any equilibrium in which all agents have non-zero contribution has to be socially optimal.

Corollary 1. *Consider an optimal equilibrium θ^{eq} . If $\theta^{\text{eq}} > 0$, then θ^{eq} is socially optimal.*

An advantage of Corollary 1 is that in many settings it is much simpler to verify that every agent has to contribute a non-zero amount at an equilibrium without computing the equilibrium directly. One such class of examples is when matrix W is a *diagonally dominant* matrix, i.e., $\sum_{j \neq i} W_{ij} < W_{ii}$ for all $i \in [k]$, in addition to satisfying the requirements of Theorem 2. In this case, every agent can satisfy their own constraint in isolation using $\vartheta_i = 1/\mu$ contribution. Therefore, in any stable equilibrium the total utility an agent will receive from all others (even at their maximum contribution of $1/\mu$) is not sufficient to meet her constraint. Therefore, every agent has a non-zero contribution in an equilibrium. This shows that the Price of Stability corresponding to diagonally dominant matrices is 1.

We defer the proofs of Theorem 6 and Corollary 1 to Appendix F. At a high level, our proofs use the duality framework and the linear program (LP 1) and convex program (CP 1).

Lastly, in the linear utilities case, it is not hard to show that any stable equilibrium is also envy-free.

Theorem 7. *When $W_{ij} < W_{ii}$ for all $i, j \in [k]$, any stable equilibrium is also envy-free.*

We defer the proof of Theorem 7 to Appendix G. Theorem 7 and Corollary 1 together highlight an advantage of optimal stable equilibria. Not only are these equilibria socially optimal for a subset of agents (and in some cases for all agents) but also they satisfy the additional property of being envy-free.

5.3. Coverage Utilities

We complement the algorithmic and structural perspective of equilibria in the linear utility case with those for the random coverage utilities. Unlike the linear utility case, both the stable feasible set and the envy-free feasible set for the random coverage utilities are non-convex, which indicates that either optimal stable equilibrium or optimal envy-free equilibrium is intractable.

Theorem 8. *There exists a random coverage example with strategy space $\Theta = \mathbb{R}_+^k$ such that Θ^{eq} is non-convex, where $\Theta^{\text{eq}} \subseteq \Theta$ is the set of all stable equilibria.*

We defer the proof to Appendix H and provide an overview of the proof of Theorem 8 here. Consider an example where there are 2 agents and both are with a uniform distribution over the instance space $\mathcal{X} = \{0, 1\}$ and $\mu_i = 3/4$ for all $i \in [2]$. Note that both e_1 and e_2 are stable equilibria, since both agents receive $3/4$ utility if either of them observe any one of the instances. Now consider a convex combination of these two strategies $(e_1 + e_2)/2$, i.e., each agent takes one sample with probability $1/2$. In this case, there is a small probability that when both agents sample they both uncover the same point. Thus, they do not receive any marginal utility from the second sample. This means that the utility that both agents receive from $(e_1 + e_2)/2$ is strictly less than $3/4$, that is, $(e_1 + e_2)/2$ is not even a feasible solution let alone a stable equilibrium. For more details refer to Appendix H.

Theorem 9. *There exists a random coverage example with strategy space $\Theta = \mathbb{R}_+^k$ such that Θ^{ef} is non-convex, where $\Theta^{\text{ef}} \subseteq \Theta$ is the set of all envy-free equilibria.*

We defer the proof to Appendix H. At a high level, considering a complete graph on 4 vertices, we let each edge correspond to one agent and put one point in the middle of every edge and one point on every vertex. Then we let each agent's distribution be a uniform distribution over \mathcal{X}_i , which

is the 3 points on agent i 's edge. In this example, we can obtain an envy-free equilibrium θ^{ef} by picking any perfect matching on this complete graph and then letting $\theta_i^{\text{ef}} = 1$ if edge i is in this matching and $\theta_i^{\text{ef}} = 0$ otherwise. However, we can show that there exists a convex combination of two envy-free equilibria corresponding to two different perfect matchings such that it is not envy-free.

6. Experimental Evaluation

To demonstrate potential issues with not considering incentives in federated learning, we compare two federated learning algorithms that account for these incentives to different extents. We consider both federated averaging (McMahan et al., 2017) and a collaborative PAC-inspired algorithm based on (Blum et al., 2017; Nguyen & Zakynthinou, 2018; Chen et al., 2018) called MW-FED. Federated averaging is envy-free as agents take the same number of samples in expectation. Unfortunately, FedAvg may find solutions that are far from any stable equilibrium. MW-FED does not explicitly guarantee envy-freeness or stability, however, we demonstrate that it produces solutions that are closer to being a stable equilibrium. This is due to the fact that it implicitly reduces the sample burden of those agents who are close to having satisfied their constraints.

Federating Algorithms At a high level, FedAvg involves sending a global model to a set of clients and requesting an updated model (from some number of updates performed by the client) based on the clients data. The server then calculates a weighted average of these updates and sets this as the new set of parameters for the model. MW-FED uses the Multiplicative Weight Update meta-algorithm and adjusts the number of samples that each agent has to contribute over multiple rounds. MW-FED takes a fixed number of samples at each round, but distributes the load across agents proportional to weights w_i^t . In the first iteration, the load is distributed uniformly between the agents, i.e., $w_i^1 = 1$. At every new iteration, the current global model is tested on each agent's holdout set. Distributions that do not meet their accuracy objective increase their w_i^t according to the Multiplicative Weight Update. A more detailed statement of the algorithm can be found in Appendix I.

EMNIST Dataset We study the balanced split of the EMNIST (Cohen et al., 2017), a character recognition dataset of 131,600 handwritten letters. EMNIST provides a variety of heterogeneous data while still remaining accessible enough to run a sufficient number of trials. We encourage further heterogeneity via a sampling technique that identifies difficult and easy points. Each agent is assigned 2000 points from some mixture of these two sets. Implicitly, this creates agents who have varying degrees of difficulty in achieving their learning objectives. From these 2000 points, 1600 are selected as the training and 400 as a validation set.

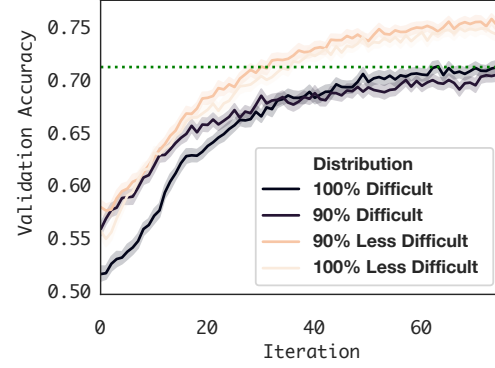


Figure 1. Each line here represents the average of 100 non-federated runs of a distribution used in this experiment. Note that the less difficult distributions reach the threshold quickly, whereas the more difficult distributions take nearly three times as long.

During the course of training, we say that a distribution's contribution is the fraction of its 1600 points that it will use during learning. That is, if an agent's contribution level is 0.01, it will take a sample of 16 points at the beginning of the optimization procedure and only uses those data when creating mini-batches.

For clarity of presentation, in these experiments we use four agents, two that have harder distributions and two that have easier distributions. Figure 1 shows the average performances of the four distributions without federation. Our observations and trends hold across larger sample sizes and with additional agents as shown in Appendix I. For training, we use a four-layer neural network with two convolutional layers and two fully-connected layers. For efficiency and to mirror real-world federated learning applications, we pre-train this model on an initial training set for 40 epochs to achieve 55% accuracy and then use federated training to achieve a 70% accuracy level for all agents. More details on the dataset and model used can be found in Appendix I.

Results. To compare the two algorithms, we consider the resulting likelihood of any agent's constraint remaining satisfied when they unilaterally reduce their contribution level. Specifically, each agent wants to attain an accuracy of 70% on their individual validation set. We chose this threshold as the easy distributions readily, individually converge above this level whereas, in our time horizon, the difficult distributions took, on average, nearly three times as long. See Figure 1 for the averaged individual performance trajectories. If an agent can drop their contribution level significantly and still attain this accuracy consistently during the optimization process, then either (a) other agents are oversampling and this agent is able to benefit from their over-allocation or (b) the agent was sampling too much to begin with relative to their requirements.

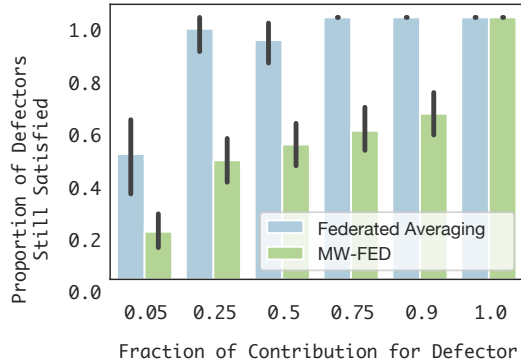


Figure 2. Comparing the likelihood that a single defector will reach their accuracy threshold at various contributions for federated averaging and MW-FED after 10 epochs. The result shows that MW-FED results in allocations that are closer to an equilibrium compared to Fedvg.

FedAvg makes no distinction between these cases. All agents contribute at an equal rate to convergence. On the other hand, MW-FED quickly reduces an agent’s contribution level when she has met her constraints, reducing her ability to oversample.

Figure 2 shows the results of FedAvg and MW-FED run on the dataset 100 times. When everyone fully contributes, 100% of these FedAvg runs satisfy the requirements of all agents by the tenth epoch. This figure compares the probability that, if a random single agent defected to a given contribution level, they would expect to have met their accuracy threshold at this point. For instance, if a single random agent only contributed 25% of their data in FedAvg, they still have a 94% chance of being satisfied by the tenth epoch. By comparison, only 45% of agents at the same contribution level would succeed in MW-FED. This is striking as is discussed further in Appendix I where, even with pre-training, none of the agents in the individual (non-federated) setting reaches 70% accuracy with 50% or less of their data. In Appendix I, we give one possible explanation for the performance of MW-FED by drawing parallels to algorithms in Section 5 that work in the linear setting.

7. Conclusion

Our paper introduced a comprehensive game theoretic framework for collaborative federated learning that considers agent incentives. Our general model extends to a wide variety of loss functions under the modest assumptions of feasibility and monotonicity. Our theoretical results and empirical observations form the first steps in what we hope will be a collective push towards designing equitable collaboration protocols that will be essential for recruiting and retaining large numbers of participating agents.

Acknowledgements

This work was supported in part by the National Science Foundations under grants CCF-1733556 and CCF-1815011, and a J.P. Morgan Chase faculty research award. Part of this work was done while Haghtalab was visiting the Simons Institute for the Theory of Computing.

References

- Agarwal, A., Dahleh, M., and Sarkar, T. A marketplace for data: An algorithmic solution. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pp. 701–726, 2019.
- Anshelevich, E., Dasgupta, A., Kleinberg, J., Tardos, É., Wexler, T., and Roughgarden, T. The price of stability for network design with fair cost allocation. *SIAM Journal on Computing*, 38(4):1602–1623, 2008.
- Arora, S., Hazan, E., and Kale, S. The multiplicative weights update method: a meta-algorithm and applications. *Theory of Computing*, 8(1):121–164, 2012.
- Balkanski, E., Syed, U., and Vassilvitskii, S. Statistical cost sharing. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, pp. 6222–6231, 2017.
- Bergen, S. E. and Petryshen, T. L. Genome-wide association studies (GWAS) of schizophrenia: does bigger lead to better results? *Current opinion in psychiatry*, 25(2):76, 2012.
- Blum, A., Haghtalab, N., Procaccia, A. D., and Qiao, M. Collaborative PAC learning. In *Advances in Neural Information Processing Systems*, pp. 2392–2401, 2017.
- Caragiannis, I., Kaklamanis, C., Kanellopoulos, P., and Kyropoulou, M. The efficiency of fair division. *Theory of Computing Systems*, 50(4):589–610, 2012.
- Chen, J., Zhang, Q., and Zhou, Y. Tight Bounds for Collaborative PAC Learning via Multiplicative Weights. In Bengio, S., Wallach, H., Larochelle, H., Grauman, K., Cesa-Bianchi, N., and Garnett, R. (eds.), *Advances in Neural Information Processing Systems 31*, pp. 3598–3607. Curran Associates, Inc., 2018.
- Cohen, G., Afshar, S., Tapson, J., and van Schaik, A. EMNIST: an extension of MNIST to handwritten letters. *CoRR*, abs/1702.05373, 2017. URL <http://arxiv.org/abs/1702.05373>.
- Donahue, K. and Kleinberg, J. Model-sharing games: Analyzing federated learning under voluntary participation. *Proceedings of the AAAI Conference on Artificial Intelligence*, 35(6):5303–5311, May

2021. URL <https://ojs.aaai.org/index.php/AAAI/article/view/16669>.
- Foley, D. K. Resource allocation and the public sector. *Yale economic essays*, 7(1):45–98, 1967.
- Ghorbani, A. and Zou, J. Data shapley: Equitable valuation of data for machine learning. In *International Conference on Machine Learning*, pp. 2242–2251. PMLR, 2019.
- Jia, R., Dao, D., Wang, B., Hubis, F. A., Hynes, N., Gürel, N. M., Li, B., Zhang, C., Song, D., and Spanos, C. J. Towards efficient data valuation based on the shapley value. In *The 22nd International Conference on Artificial Intelligence and Statistics*, pp. 1167–1176. PMLR, 2019.
- Kang, J., Xiong, Z., Niyato, D., Xie, S., and Zhang, J. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 6(6): 10700–10714, 2019.
- Kingma, D. P. and Ba, J. Adam: A Method for Stochastic Optimization. *arXiv:1412.6980 [cs]*, January 2017. URL <http://arxiv.org/abs/1412.6980>. arXiv: 1412.6980.
- Li, T., Sanjabi, M., Beirami, A., and Smith, V. Fair resource allocation in federated learning. *arXiv preprint arXiv:1905.10497*, 2019.
- Lin, J., Du, M., and Liu, J. Free-riders in federated learning: Attacks and defenses. *arXiv preprint arXiv:1911.12560*, 2019.
- Lyu, L., Xu, X., Wang, Q., and Yu, H. Collaborative fairness in federated learning. In *Federated Learning*, pp. 189–204. Springer, 2020.
- McMahan, B. and Ramage, D. Federated learning: Collaborative machine learning without centralized training data. *Google Research Blog*, 3, 2017.
- McMahan, B., Moore, E., Ramage, D., Hampson, S., and y Arcas, B. A. Communication-efficient learning of deep networks from decentralized data. In *Artificial Intelligence and Statistics*, pp. 1273–1282. PMLR, 2017.
- Nash, J. Non-cooperative games. *Annals of mathematics*, pp. 286–295, 1951.
- Nguyen, H. and Zakynthinou, L. Improved algorithms for collaborative pac learning. *Advances in Neural Information Processing Systems*, 31:7631–7639, 2018.
- Plotkin, S. A., Shmoys, D. B., and va Tardos. Fast approximation algorithms for fractional packing and covering problems. *Mathematics of Operations Research*, 20(2): 257–301, 1995. ISSN 0364765X, 15265471.
- Powell, K. NVIDIA clara federated learning to deliver ai to hospitals while protecting patient data. <https://blogs.nvidia.com/blog/2019/12/01/clara-federated-learning/>, 2019.
- Sim, R. H. L., Zhang, Y., Chan, M. C., and Low, B. K. H. Collaborative machine learning with incentive-aware model rewards. In *International Conference on Machine Learning*, pp. 8927–8936. PMLR, 2020.
- Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1):1929–1958, 2014.
- Varian, H. R. Equity, envy, and efficiency. *Journal of Economic Theory*, 9(1):63–91, 1974. ISSN 0022-0531.
- Wen, Y., Li, W., Roth, H., and Dogra, P. Federated learning powered by NVIDIA Clara. Technical report, December 2019. URL <https://developer.nvidia.com/blog/federated-learning-clara/>.
- Yu, H., Liu, Z., Liu, Y., Chen, T., Cong, M., Weng, X., Niyato, D., and Yang, Q. A fairness-aware incentive scheme for federated learning. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, pp. 393–399, 2020.
- Zhang, J., Li, C., Robles-Kelly, A., and Kankanhalli, M. Hierarchically fair federated learning. *arXiv preprint arXiv:2004.10386*, 2020.