Optimality and Stability in Federated Learning

Lokesh Mohanty
Department of Computational and Data Sciences
Indian Institute of Science
Bangalore, 560012
lokeshm@iisc.ac.in

Abstract

In the distributed learning paradigm known as federated learning, multiple agents who each have access to just local data work together to collaboratively learn a global model. There has been a recent surge in research in this field trying to ensure socially beneficial qualities like total error as well as an increase in the accuracy rates of federated learning. But there is limited study on the stability and optimality of federated learning. In this project, we will study game-theoretic approaches to model federated learning and study the optimality and stability in federated learning. In this work, we will mainly study the results by ([7]). ([7]) has used a game-theoretic approach to study the optimality and the relation between optimality and stability in federated learning. Existing work has also interpreted federated learning as a hedonic game in which agents who minimise errors form federating coalitions. Using this, the authors of this study published a paper before this on a theoretical study on the stability of federated learning and also gave a model for it. Since work prior to this doesn't say how far from the optimal, the stable solutions are, ([7]) tries to find a relation between the stability and optimality of federated learning. It demonstrates that there exists some stable arrangement that is optimal and also gives a upper bound for the worst stable arrangement using the notion of Price of Anarchy.

1 Introduction

In recent years, due to the boom in machine learning and data science, a huge amount of data is being used to train machine learning models. But in real world situations, data is distributed over different locations and often expensive to gather to a central location. There are also other challenges such as data privacy, data format, missing features, etc.,.

For example, consider a group of hospitals and patient information being their data. The data in each hospital may be less which can lead to high variance if a machine learning model is trained at each hospital separately which is less likely to capture the data distribution. To fix this, data from all the hospitals can be transfered to a central location and then a machine learning model can be trained on it. This decreases the variance but brings several other issues. Some of them being the huge cost of data transfer from all the hospitals, maintaining a single location with large computing capabality, different hospitals having different data format and hospitals not preferring to share the private information of the patients (data privacy).

The problem with data privacy and huge data transfer can probably be handled by hashing the data before transfer but it adds its own problems. Losing interpretability is a major problem and mismatch of data format makes the training useless.

([20]) solves this problem using federated learning which is a novel distributed learning paradigm. In this, instead of transfer of data, machine learning models are trained at each of the separate locations

35th Conference on Neural Information Processing Systems (NeurIPS 2021).

(hospitals in our example) and then the model parameters that are learnt are shared to a common location where all the parameters are averaged to form a single global model which every hospital can use. There are many studies in federated learning like ([16, 12, 17]).

However, some studies have also shown that the single global model that is trained using federated learning may not be the best option for some agents ([23, 3, 21, 15]). This is can be caused due to the actual distributions of each agent being different. If the difference between the distributions are large, then the global model trained might actually perform worse than the local model. It is also likely that the agents will have different amount of data leading to global model shifting towards the agent with large amount of data.

To handle this, instead of combining all the models, each agent can be given the choice to combine their model or not based on their local model performance and the combined model performance. Here every agent simultaneously tries to find the best federating group to join. ([11]) has formulated this as a hedonic game where each agent faces some cost for joining a coalition(federating group). The goal of such work is to find the groups that are stable to deviations or are in equilibrium. Since a hedonic game may not have any such stable arrangements, analysis of stability can add value to the research and give insights on incentives of the federating agents.

This also leaves a lot questions. Stability of an arrangement can be studied by assuming individually rational agents and some metric like the model error. However, this is a self-interested goal. The society as a whole would also like to minimize the overall error. In the hospitals example, the state/country would like to minimize the overall error of all the hospitals. In game theory, this can be studied by analysis of optimality.

Overall, this leads to requirement of study on the self-interested goals of the individual agents (stability) and minimization of the overall error (optimality). An interesting study would be to bound the optimality given that the arrangement of agents is stable. This can be achieved by the concept of Price of Anarchy which can be used to study the relation between stability and optimality of an arrangement ([13, 22]). Price of Anarchy (PoA) is the ratio of the highest cost/error stable arrangement to the lowest cost/error stable arrangement. Where the lowest cost stable arrangement is the optimal arrangement. We can see that the lower bound of PoA is 1 as in the best case, the highest cost stable arrangement and the lowest stable arrangement have the same cost. But finding the upper bound it not so trivial. In federated learning, there has been a lot of study on stability of agents but there are hardly any systematic studies on optimality of an arrangement.

In this project, we will mainly the study the results of ([7]). ([6]) gives a theoretical model of federating learning with closed-form solutions for errors/cost derived by an agent for joining a coalition. It analyzes the stability of coalitions using this model. Using the results of ([6]), ([7]) provides an efficient algorithm for finding the optimal arrangement. After that, it proves a constant upper bound for Price of Anarchy showing that the highest cost stable arrangement will be no more than 9 times the lowest cost stable arrangement (optimal arrangement). While coming up with this upper bound of 9 for Price of Anarchy, ([7]) shows that there always exists an optimal arrangement which is stable, then there exist some stable arrangement that are not stable and finally that the worst stable arrangement has cost no more than 9 times that of the best arrangement. The proofs given by these two studies are modular and also illuminate multiple properties of the federated learning game. Hence, these could be useful for further investigating the federated learning model.

First we will review the related work in this field of federated learning using game-theoretic approaches in Section 2. Then we will study in depth the work of ([7]) and their implications in Section 3. Finally we will summarize our extension of this work and conclude in Section 4.

2 Related Work

As mentioned earlier, federated learning has recently seen rapid growth in both applied and theoretical research. Now there are also many studies applying game theory to federated learning. In this section we will highlight some of the studies that are related to this project.

The notion that agent's true models may change due to non-i.i.d. data being created across many agents is widely accepted in the federated learning studies. For example ([23, 3]), empirical evidence shows that federated learning, particularly privacy-related additions, can result in a substantial divergence in error rates. Some methods have been created specifically to address this issue. Hierarchical federated learning, for example, adds another layer of hierarchical structure to federated learning, which might be used to minimise latency or to group together similar agents ([18, 19]).

An earlier work by ([11]) (Incentive Mechanism Design for Federated Learning: Hedonic Game Approach) formulates federated learning as a hedonic game where each agent has the option to choose which coalition to join and is given the cost which it would have to incur on joining it. It also gives conditions for Nash equilibrium. Using this, Donahue and Kelinberg in their study (Model-sharing Games: Analyzing Federated Learning Under Voluntary Participation)([6]) studied stability of a coalition with the assumption that a federation is stable if an agent's error decreases by joining it.

The focus of [6] is defining a theoretical model of federated learning and analyzing the stability of such an arrangement. As such, it focuses solely on individual incentives and completely omitted any analysis of overall societal welfare. Whereas ([7]) focuses on discussions of optimality (overall welfare) and Price of Anarchy, questions that are completely distinct from ([6]). This study gave a model for three methods of federation, one being the vanilla or uniform and two other models of domain adaptation. This work studies stability of federated learning for three types of federations. The first one being the case where every agent joins the global coalition irrespective of the cost derived from it. The second one being the case where there is a single coalition but every agent has an option to join or not join it. This is termed as coarse-grained federation. The third one being the most general, multiple coalitions can be formed with every agent having the option to join any coalition or not join any at all.

There are many other studies going on in this area which use the results of this study. Like ([8]) studies and formulates models of fairness in federated learning, ([9]) models clients behaviour in a network using federated learning, ([10]) is very similar to this work but it tries to find a collaboration equilibrium instead using the results of this study. There are also many studies whose results can be combined with this. ([4]) for example analyzes fairness and efficiency in sampling additional points for federated learning while ([14]) analyzes incentives for agents to contribute computational resources in federated learning while using an auction approach. There is also a study by ([1]) which uses a game theoretic approach towards coalition formation in cloud computing, but with the aim of minimizing some cost besides error like electricity usage.

3 Main Contributions

The current study ([7]), inorder to construct a framework for stability and optimality in federated learning, establishes an optimality concept based on the average error of federating agents. In first part of the study, it constructs an efficient algorithm for calculating an optimal arrangement and also the proof of its optimality.

3.1 Model and Assumptions

To construct an efficient algorithm for calculating optimal arrangement, we need a theoretical model of federation. We state below the notations that we will be using

- Total number of agents $\rightarrow M$
- Number of data points shared by each agent $i \rightarrow n_i$
- True local parameters of agent $i \rightarrow \theta_i$
- True local distribution of agent $i \rightarrow g(\theta_i)$
- Local estimate of agent $i \rightarrow g(\hat{\theta}_i)$
- Local error of agent $i \rightarrow err_i(\{i\})$
- A set of agents federating together (coalition) $\rightarrow C$
- Error of agent i in a coalition $C \rightarrow err_i(C)$
- Collection of coalitions that partitions the M agents $\rightarrow \Pi$

Combination of local estimation of parameters of a set of agents forming a coalition C is goverened by the weighted average of their parameters.

$$\hat{\theta}_C = \frac{1}{\sum_{i \in C} n_i} . \sum_{i \in C} n_i . \hat{\theta}_i \tag{1}$$

From this we can see that, the coalition parameters are weighted more towards agents with large amount of data. This will lead to lower error for agents with more number of datapoints. This weighted average method of calculating the coalition parameters estimate is commonly used in federated learning ([20]). This method is also called "vanilla" federated learning as it is the most straightforward method. Alternative ways of federation can be considered to incentivize certain invidual agents or to make it more fair for the agents with lower number of data points. This is also called domain adaptation. Using alternative ways of federation may lead to different Price of Anarchy bounds. The vanilla federated learning is the only one considered in ([7]). Whereas ([**?**]) also studies two models of domain adaptation for stability analysis.

3.2 Theoretical model of federation

Both applied and theoretical analysis have been done in federated learning. But to derive an efficient algorithm to find an optimal arrangement, a model that gives exact errors for each agent is required. Such a model was developed earlier by the same authors in ([6]). ([6]) provides a closed-form error value for each agent in a coalition. ([6]) was focused on deriving a model for federating learning and analyzing the stability of federating coalitions while ([7]) is focused on analyzing optimality and Price of Anarchy of federating coalitions.

Lemma 1 (Lemma 4.2, from [6])**.** *Consider a mean estimation task as follows: agent j is trying to learn its true mean θ_j. It has access to n_j samples drawn i.i.d. $Y \sim \mathcal{D}_j(\theta_j, \epsilon_j^2)$, a distribution with mean θ_j and variance ϵ_j^2. Given a population of agents, each has drawn parameters $(\theta_j, \epsilon_j^2) \sim \Theta$ from some common distribution Θ. A coalition C federating together produces a single model based on the weighted average of local means (Eq. 1). Then, the expected mean squared error agent j experiences in coalition C is:*

$$err_j(C) = \frac{\mu_e}{\sum_{i \in C} n_i} + \sigma^2 \cdot \frac{\sum_{i \in C, i \neq j} n_i^2 + \left(\sum_{i \in C, i \neq j} n_i\right)^2}{\left(\sum_{i \in C} n_i\right)^2} \tag{2}$$

where $\mu_e = \mathbb{E}_{(\theta_i, \epsilon_i^2) \sim \Theta}[\epsilon_i^2]$ (the average noise in data sampling) and $\sigma^2 = Var(\theta_i)$ (the average distance between the true means of agents).

[6] also analyzes a linear regression game with a similar cost function, however, in this work we will focus only on the mean estimation game.

The technical assumptions that are made are:

- $\{n_i\}$ is fixed and known by all
- Parameters μ_e, σ^2 are approximately known (the critical threshold $\frac{\mu_e}{\sigma^2}$ in particular is known)
- Agents do not know anything else about their own true parameters θ_i or the parameters of other agents
- Every agent has a goal of obtaining a model with low expected test error on its personal distribution
- Federating coordinator is motivated to minimize some notion of total cost, but is otherwise impartial.

3.3 Defining optimality

With the theoretical model of federation from Lemma 1, we can start with finding and analyzing an optimal arrangement. We will start with the objective function of the most federated learning papers [20]:

$$\min_{\theta} err_w(\theta) = \sum_{i=1}^{M} p_i \cdot err_i(\theta) =^* \frac{1}{\sum_{i=1}^{M} n_i} \sum_{i=1}^{M} n_i \cdot err_i(\theta)$$

While the weights can be any $p_i > 0, \sum_{i=1}^{M} p_i = 1$, the $*$ equality reflects the common setting where they are taken to be the empirical average. In this work, we will take the empirical average as our cost function:

Definition 1. *A coalition partition* Π *is optimal if it minimizes the weighted sum of errors across agents, as defined below:*

$$f_w(\Pi) = \sum_{C \in \Pi} f_w(C) = \sum_{C \in \Pi} \sum_{i \in C} n_i \cdot err_i(C)$$

We will say that a coalition partition Π *is in* OPT *if it achieves minimal cost. Note that multiple partitions may achieve minimal cost, so* OPT *is a set of partitions.*

Because Π is a disjoint partition over the M agents, $f_w(\Pi)$ is simply the error $err_w(\theta)$ scaled by a constant. Therefore, minimizing $f_w(\Pi)$ is equivalent to minimizing the weighted average of errors.

Some machine learning papers modify the empirical average objective to achieve other goals. For example, [15, 21] consider variants where this goal is re-weighted in order to achieve certain fairness goals.

All of the above analysis holds for any model of federated learning. Lemma 2, below, gives the specific form of cost for federated learning using the model from [6]. The remaining analysis in this paper will assume this cost function.

Lemma 2. *Consider a partition* Π *made up of coalitions* $\{C_i\}$*. Then, using the error form given in Equation 2, the total cost of* Π *is given by*

$$f_w(\Pi) = \sum_{C \in \Pi} \left\{ \mu_e + \sigma^2 \cdot N_C - \sigma^2 \frac{\sum_{i \in C} n_i^2}{N_C} \right\}$$

The two most common arrangements in machine learning tasks are local learning (which we will denote by π_l) and the federation in the *grand coalition* (π_g), where all of the agents are federating together in a single coalition. However, Lemmas 3 and 4 demonstrate that either of these could could perform arbitrarily poorly as compared the cost-minimizing (optimal) arrangement.

Lemma 3. $\forall \rho > 1$*, there exists a setting where local learning results in average error more than* ρ *times higher than optimal:* $\frac{f_w(\pi_l)}{f_w(OPT)} > \rho$*.*

Lemma 4. $\forall \rho > 1$*, there exists a setting where federating in the grand coalition results in average error more than* ρ *times higher than optimal:* $\frac{f_w(\pi_g)}{f_w(OPT)} > \rho$*.*

We can see that, finding a partition of agents that minimized the total error is computationaly very expensive. There are exponentially many possibilities for partitions and the above two lemmas show that either of the common choices can be far from optimal. In the next subsection an efficient algorithm to find the optimal arrangement will be derived.

3.4 Deriving an algorithm for optimal arrangement

The main contribution of this section is Theorem 1 gives an algorithm for minimizing the total weighted error of the federating agents.

Theorem 1. *Consider a set of agents* $\{n_i\}$*. An optimal partition* Π *can be created as follows: first, start with every agent doing local learning. Then, begin by grouping the agents together in ascending order of size, stopping when the first agent would increase its error by joining the coalition from local learning. Then, the resulting partition* Π *is optimal.*

Though the algorithm in Theorem 1 is straightforward, proving the optimality of the resulting partition Π requires several sub-lemmas. Each sub-lemma is a building-block that describes certain operations that either increase or decrease total cost. The proof of Theorem 1 largely consists of sequentially using these sub-lemmas in order to demonstrate the optimality of the calculated partition.

Statement and description of supporting lemmas First, Lemma 5 demonstrates a close relationship between movements of agents that reduce total cost and movements of agents that are in that agent's self-interest (recall that agents always wish to minimize their expected error). Specifically, it shows that a agent wishes to join a coalition from local learning if and only if that move would reduce total cost for the entire partition.

Lemma 5 (Equivalence of agent preference and reducing cost)**.** *Take any coalition Q and any agent j. Then, a agent wishes to join that coalition (from local learning) if and only if doing so would reduce total cost. That is,*

$$f_w(\{n_j\}) + f_w(Q) \geq f_w(\{n_j\} \cup Q) \quad \Leftrightarrow \quad err_j(\{n_j\}) \geq err_j(\{n_j\} \cup Q)$$

Next, Lemma 6 shows that "swapping" the roles of two agents (one doing local learning, one federating in a coalition) reduces total cost when the larger agent is removed to local learning.

Lemma 6 (Swapping)**.** *Take any set Q including a agent $n_j > n_k$, where the agent n_k is doing local learning. Then, swapping the roles of agents k and j always decreases total cost.*

$$f_w(Q \cup \{n_j\}) + f_w(\{n_k\}) > f_w(Q \cup \{n_k\}) + f_w(\{n_j\})$$

Lemmas 7 and 8 give results for when agents are incentivized to leave or join a particular coalition: they show that such incentives are monotonic in the size of the agent. By Lemma 5, these results also show the monotonicity of cost-reducing operations. Note that these lemmas are not equivalent: they differ in whether the reference agent j is already in the coalition or not.

Lemma 7 (Monotonicity of joining)**.** *If a agent of size n_j would prefer local learning to joining a coalition Q, then any agent of size $n_k \geq n_j$ also prefers local learning to joining the same coalition. That is, for $n_k \geq n_j$,*

$$err_j(Q \cup \{n_j\}) \geq err_j(\{n_j\}) \quad \Rightarrow \quad err_k(Q \cup \{n_k\}) \geq err_k(\{n_k\})$$

Conversely, if a agent j wishes to join Q, then any other agent of size $n_k \leq n_j$ would have also wanted to join. That is, for $n_j \geq n_k$,

$$err_j(Q \cup \{n_j\}) \leq err_j(\{n_j\}) \quad \Rightarrow \quad err_k(Q \cup \{n_k\}) \leq err_k(\{n_k\})$$

Lemma 8 (Monotonicity of leaving)**.** *Take any coalition Q. Then, if any agent $j \in Q$ of size n_j wishes to leave Q for local learning, then any agent of size $n_k \geq n_j$ also wishes to leave for local learning. That is, for $n_k \geq n_j$*

$$err_j(Q) \geq err_j(\{n_j\}) \quad \Rightarrow \quad err_k(Q) \geq err_k(\{n_k\})$$

Conversely, if a agent $j \in Q$ of size n_j does not *wish to leave Q for local learning, then any agent $k \in Q$ of size $n_k \leq n_j$ also does not wish to leave. That is, for $n_k \leq n_j$*

$$err_j(Q) \leq err_j(\{n_j\}) \quad \Rightarrow \quad err_k(Q) \leq err_k(\{n_k\})$$

All of the above lemmas have analyzed situations where a single agent is moving between coalitions. Lemma 8 analyzes cases where multiple agents are rearranged simultaneously. Specifically, it provides an algorithm for combining together two separate groups (and then removing certain agents) that is guaranteed to keep constant or reduce total cost.

Lemma 9 (Merging)**.** *Consider two groups of agents, P, Q. First, merge together the two groups to form $P \cup Q$. Then, remove agents from $P \cup Q$ to local learning, removing them in descending order of size. Stop removing agents when the first agent would prefer to stay (removing it would increase its error). Then, this overall process maintains or decreases total error. In other words,*

$$f_w(Q) + f_w(P) \geq f_w(\{Q \cup P\} \setminus L) + \sum_{i \in L} f_w(\{n_i\}) \tag{3}$$

where L is the set of large agents removed in descending order of size. The inequality is strict so long as the final structure is not identical to the first, up to renaming of agents, and it is not *the case that all the agents have the exact same size.*

The proof of Theorem 1 is given simply by applying the lemmas sequentially to show that any other partition Π' can be converted to the described partition Π through a series of operations that decrease or hold constant total cost.

Coalition structure	$err_a(\cdot), n_a = 1$	$err_b(\cdot), n_b = 8$	$err_c(\cdot), n_c = 15$	$f_w(\Pi)$	$err_w(\Pi)$
$\{a, \}, \{b\}, \{c\}$	10	1.25	0.667	30	1.25
$\{a\}, \{b, c\}$	10	1.285	0.677	30.435	1.268
$\{a, c\}, \{b\}$	2.382	1.25	0.633	21.875	0.911
$\{a, b\}, \{c\}$	2.691	1.136	0.667	21.778	0.907
$\{a, b, c\}$	1.834	1.253	0.670	21.917	0.913

Table 1: Example with $\mu_e = 10, \sigma^2 = 1$ example with three agents of size $n_a = 1, n_b = 8, n_c = 15$. Note that $\{a, b\}, \{c\}$ minimizes total cost, but is not individually stable: agent a wishes to leave its coalition to join agent c, which welcomes that agent joining it. This produces $\{a, c\}, \{b\}$, which is the only individually stable arrangement, giving a Price of Anarchy value of $21.875/21.778 = 1.0045$.

3.5 Price of Anarchy

The previous section defined the "optimality" of a federating arrangement as its average error, and additionally provided an efficient algorithm to calculate a lowest-cost arrangement. Given that much of prior work ([6, 11]) has studied the stability of cooperative games induced by federated learning, the next natural question is to study the relationship between stability and optimality. This section analyzes this relationship, using the canonical game theoretic tools of Price of Anarchy and Price of Stability. All proofs for this section are in Appendix **??**.

First, we will define the notions of stability under analysis, which are all drawn from standard cooperative game theory literature ([5]). A partition of agents Π is *core stable* if there does not exist a set of agents that all would prefer leave their location in Π and form a coalition together. A partition is *individually stable* (IS) if there does not exist a single agent i that wishes to join some existing coalition C, where all members of C weakly prefer that i join. Our results will primarily use the notion of individual stability.

As a reminder, the Price of Anarchy (PoA) is the ratio between the worst (highest-cost) stable arrangement and the best (lowest-cost) arrangement. The Price of Stability is the ratio of the best stable arrangement and the best overall arrangement (regardless of if it is stable or not) ([2]). Note that the Price of Stability is 1 when there exists an optimal arrangement that is also stable.

First, we will show that for certain ranges of parameter space, the Price of Anarchy and/or Price of Stability are equal to 1. Specifically, Lemma 10 shows that when all agents have relatively few samples (no more than $\frac{\mu_e}{\sigma^2}$ each), the grand coalition π_g is core stable, implying a Price of (Core) Stability of 1. Recall that μ_e and σ^2 are parameters of the federated learning model reflecting the average noise of the data and the average dissimilarity between federating agents, respectively.

Lemma 10. *For a set of agents with $n_i \leq \frac{\mu_e}{\sigma^2}$ $\forall i$, the grand coalition π_g is always core stable.*

On the other hand, Lemma 11 shows that when all agents have relatively many samples (at least $\frac{\mu_e}{\sigma^2}$ each), every core or individually stable arrangement is also optimal, which means that the Price of Anarchy for this situation is 1.

Lemma 11. *For a set of agents with $n_i \geq \frac{\mu_e}{\sigma^2}$ $\forall i$, any arrangement that is core stable or individually stable is also optimal.*

However, it is *not* the case that either the Price of Stability or Price of Anarchy is always 1. Table 1 contains an example demonstrating this: there exists a simple three-agent case where the optimal arrangement is not individually stable. However, the Price of Anarchy value here is quite small, which suggests the prospect that the Price of Anarchy in general could be bounded.

The main result of this section is Theorem 2, which proves a Price of Anarchy bound of 9 for this problem: the cost of the highest stable arrangement is no more than 9 times the cost of the optimal (lowest cost) arrangement.

Theorem 2 (Price of Anarchy)**.** *Denote Π_M to be a maximum-cost individually stable (IS) partition and Π_{opt} to be an optimal (lowest-cost) partition. Then,*

$$PoA = \frac{f_w(\Pi_M)}{f_w(\Pi_{opt})} \leq 9$$

In Theorem 2, the numerator is the cost of Π_M, a maximum-cost partition, and the denominator is Π_{opt}, an optimal (lowest-cost) partition. Recall that Definition 1 gives the cost of an arrangement as the weighted sum of the errors of the respective agents. Therefore, to get an upper bound on the Price of Anarchy, we will upper bound the errors agents experience in Π_M and lower bound on the error agents experience in Π_{opt}.

Summary of proof technique Again, this section will show how the larger theorem is the result of several lemmas that act as building blocks. In particular, the lemmas will take two separate approaches towards creating the bound. Lemmas of the first type (12, 13, 14) all provide upper or lower bounds on the errors certain agents can experience. These conditions depend on the size of the agent (how many samples it has) and the size of the group it is federating with (how many samples in total the rest of the coalition has). For example, Lemmas 12 and 13 taken together show that a agent with at least $\frac{\mu_e+\sigma^2}{2\sigma^2}$ samples has a worst-case error no more than 2 times its best-case error. The same pair of lemmas give a multiplicative bound of 9 for agents with numbers of samples that falls between $\frac{\mu_e}{9\cdot\sigma^2}$ and $\frac{\mu_e+\sigma^2}{2\sigma^2}$. Finally, Lemmas 14 and 13 together give a factor of 7.5 for agents with fewer than $\frac{\mu_e}{9\cdot\sigma^2}$ samples that are federating with other agents of total size at least $\frac{\mu_e}{3\cdot\sigma^2}$. Taken together, these errors show that, for almost all cases, the highest error a agent experiences is no more than 9 times higher than the lowest error it might experience.

The final case that needs to be addressed is when a agent of size $\leq \frac{\mu_e}{9\cdot\sigma^2}$ is federating in a group with other agents of total size $\leq \frac{\mu_e}{3\cdot\sigma^2}$. Lemma 15 handles this last case by an argument around stability. Specifically, it shows that any agents in such an arrangement can only be stable if all of them are grouped together into a single federating coalition. In the proof of Theorem 2, this result ends up enabling an additive factor to the Price of Anarchy bound, which is absorbed into the other factors for a total Price of Anarchy value of 9.

Statement and description of supporting lemmas Next, we will walk through each lemma specifically. Lemma 12 gives an *upper* bound of $\frac{\mu_e}{n_i}$ on the error any agent experiences in Π_M.

Lemma 12. *If Π_M is a maximum-cost IS partition, then $err_i(\Pi_M) \leq \frac{\mu_e}{n_i}$ for all agents i.*

Proof. Because Π_M is individually stable, every agent must get error no more than the error it would receive alone (doing local learning). By Lemma 1 with $C = n_i$, a agent with samples n_i agent gets error $\frac{\mu_e}{n_i}$ alone. □

Next, Lemma 13 provides *lower* bounds on the error a agent can receive in Π_{opt}. It does this by bounding the minimum error a agent could get in any arrangement. Again, because the cost of Π_{opt} is simply the weighted sum of errors of each individual agent, this helps to upper bound the Price of Anarchy. First, Lemma 13 shows that for agents with at least $\frac{\mu_e+\sigma^2}{2\sigma^2}$ samples, the lowest possible error it could experience is $\frac{1}{2}\cdot\frac{\mu_e}{n_j}$, which is a factor of 2 off from its worst-case error in Lemma 12. For agents with fewer samples than $\frac{\mu_e+\sigma^2}{2\sigma^2}$, Lemma 13 says that the lowest error a agent could experience is σ^2. This means that the ratio between the two errors is lower than 9 so long as $n_j \geq \frac{\mu_e}{9\cdot\sigma^2}$. Therefore, in order to get a factor of 9 bound for the overall Price of Anarchy, we need to handle the case of agents with size $\leq \frac{\mu_e}{9\cdot\sigma^2}$, when agents have very few samples.

Lemma 13. *Consider a agent n_j and any set of agents C. Then, we can lower bound the error agent j recieves by federating with C:*

$$err_j(C \cup \{n_j\}) \geq \begin{cases} \frac{1}{2}\cdot\frac{\mu_e}{n_j} & n_j \geq \frac{\mu_e+\sigma^2}{2\sigma^2} \\ \sigma^2 & \textit{otherwise} \end{cases}$$

Lemma 14 is the first of two lemmas handling the case of agents with very few samples. It shows that, if a agent of size $\leq \frac{\mu_e}{3\cdot\sigma^2}$ is federating with a set of agents of total size at least $\frac{\mu_e}{3\cdot\sigma^2}$, it is possible to *upper* bound on the error of agents in Π_M by $7.5\cdot\sigma^2$. Given the lower bound of σ^2 in Lemma 13, these together show that there is a ratio of 7.5 at most between the error this agent experiences in its best and worst-case arrangements.

Lemma 14. *Consider a agent j federating with a coalition C. If the total number of samples N_C is at least $\frac{\mu_e}{3\sigma^2}$, then $err_j(C \cup \{n_j\}) \leq 7.25\cdot\sigma^2$.*

However, Lemma 14 does not handle one situation: what if a agent of size $\leq \frac{\mu_e}{9 \cdot \sigma^2}$ is federating with a group of agents of total size $\leq \frac{\mu_e}{3 \cdot \sigma^2}$? Lemma 15 addresses this last case: it shows that the only such arrangement that is stable is one where all such agents are grouped together into a single arrangement. Note that this lemma is itself should not be obvious: it is composed of multiple sub-lemmas which are stated and proved in the appendix. The fact that there can be only one group of such agents is used in the Theorem 2 to create an overall bound of 9.

Lemma 15. *Consider an arrangement of agents, all of size $\leq \frac{\mu_e}{3\sigma^2}$, where at least one agent is in a federating cluster where the total mass of its partners is no more than $\frac{\mu_e}{3\sigma^2}$. Then, the only stable arrangement of these agents is to have all of them federating together.*

The full proof of Theorem 2 uses these lemmas collectively in order to get an overall Price of Anarchy bound of 9, showing that the worst individually stable arrangement has total cost no more than 9 times the optimal cost.

4 Conclusion

We have studied various works which are related to optimality and stability in federated learning and summarized them. We deeply studied the paper ([7]) which gives an algorithm to find the optimal arrangement and gives a constant-factor Price of Anarchy bound for optimality which quantifies the relation between individual incentives and overall societal goals. This is a theoritical study and hence the results might be different in acutal practice. The optimality bound that ([7]) has given has some assumptions on what is optimal. This need not be true for all cases, and where these assumptions are not valid this bound loses its value.

This study is not restricted to a particular application and hence can be used for any application. Though different definitions of the cost could result in different Price of Anarchy bounds. Other than the optimality bound, the construction of the framework for optimality and stability can be helpful for designing more complex models of federation with different definitions of optimality like fairness.

References

[1] C. Anglano, M. Canonico, Paolo Castagno, Marco Guazzone, and M. Sereno. A game-theoretic approach to coalition formation in fog provider federations. *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 123–130, 2018.

[2] Elliot Anshelevich, Anirban Dasgupta, Jon Kleinberg, Éva Tardos, Tom Wexler, and Tim Roughgarden. The price of stability for network design with fair cost allocation. *SIAM Journal on Computing*, 38(4):1602–1623, 2008.

[3] Eugene Bagdasaryan and Vitaly Shmatikov. Differential privacy has disparate impact on model accuracy, 2019.

[4] Avrim Blum, Nika Haghtalab, Richard Lanas Phillips, and Han Shao. One for one, or all for all: Equilibria and optimality of collaboration in federated learning. *arXiv preprint arXiv:2103.03228*, 2021.

[5] Anna Bogomolnaia and Matthew O. Jackson. The stability of hedonic coalition structures. *Games and Economic Behavior*, 38(2):201 – 230, 2002. ISSN 0899-8256. doi: https://doi.org/10.1006/game.2001.0877. URL http://www.sciencedirect.com/science/article/pii/S0899825601908772.

[6] Kate Donahue and Jon Kleinberg. Model-sharing games: Analyzing federated learning under voluntary participation. *AAAI 2021*, 2021. URL https://arxiv.org/abs/2010.00753.

[7] Kate Donahue and Jon Kleinberg. Optimality and Stability in Federated Learning: A Game-theoretic Approach. *NeurIPS 2021*, 2021. URL https://arxiv.org/abs/2106.09580.

[8] Kate Donahue and Jon Kleinberg. Models of fairness in federated learning *CoRR*, 2021. URL https://arxiv.org/abs/2112.00818.

[9] Hu, S., Ngo, D. D., Zheng, S., Smith, V., and Wu, Z. S. Federated Learning as a Network Effects Game. *CoRR*, 2021. URL https://arxiv.org/abs/2302.08533.

[10] Cui, S., Liang, J., Pan, W., Chen, K., Zhang, C., & Wang, F. Collaboration equilibrium in federated learning. *CoRR*, 2021. URL https://arxiv.org/abs/2108.07926.

[11] Cengis Hasan. Incentive mechanism design for federated learning: Hedonic game approach, 2021.

[12] Peter Kairouz, H. Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, 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, Adrià Gascón, 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 Konečný, Aleksandra Korolova, Farinaz Koushanfar, Sanmi Koyejo, Tancrède Lepoint, Yang Liu, Prateek Mittal, Mehryar Mohri, Richard Nock, Ayfer Özgür, Rasmus Pagh, Mariana Raykova, Hang Qi, Daniel Ramage, Ramesh Raskar, Dawn Song, Weikang Song, Sebastian U. Stich, Ziteng Sun, Ananda Theertha Suresh, Florian Tramèr, 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, 2019.

[13] Elias Koutsoupias and Christos Papadimitriou. Worst-case equilibria. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 404–413. Springer, 1999.

[14] Tra Huong Thi Le, Nguyen H. Tran, Yan Kyaw Tun, Minh N. H. Nguyen, Shashi Raj Pandey, Zhu Han, and Choong Seon Hong. An incentive mechanism for federated learning in wireless cellular network: An auction approach. *IEEE Transactions on Wireless Communications*, pages 1–1, 2021. doi: 10.1109/TWC.2021.3062708.

[15] Tian Li, Maziar Sanjabi, Ahmad Beirami, and Virginia Smith. Fair resource allocation in federated learning, 2019.

[16] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3):50–60, May 2020. ISSN 1558-0792. doi: 10.1109/msp.2020.2975749. URL `http://dx.doi.org/10.1109/MSP.2020.2975749`.

[17] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y. C. Liang, Q. Yang, D. Niyato, and C. Miao. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys Tutorials*, 22(3):2031–2063, 2020. doi: 10.1109/COMST.2020.2986024.

[18] Tao Lin, Sebastian U. Stich, Kumar Kshitij Patel, and Martin Jaggi. Don't use large mini-batches, use local sgd, 2018.

[19] Lumin Liu, Jun Zhang, S.H. Song, and Khaled B. Letaief. Client-edge-cloud hierarchical federated learning. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Jun 2020. doi: 10.1109/icc40277.2020.9148862. URL `http://dx.doi.org/10.1109/icc40277.2020.9148862`.

[20] H. Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data, 2016.

[21] Mehryar Mohri, Gary Sivek, and Ananda Theertha Suresh. Agnostic federated learning, 2019.

[22] Christos Papadimitriou. Algorithms, games, and the internet. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 749–753, 2001.

[23] Tao Yu, Eugene Bagdasaryan, and Vitaly Shmatikov. Salvaging federated learning by local adaptation, 2020.