Collaborative Machine Learning with Incentive-Aware Model Rewards

Contributions Of The Paper

1. Proposing a data valuation model using the information gain on model parameters given the data.

2. Defining new conditions for incentives

3. Injecting gaussian noise into aggregated data from multiple parties and optimising the noise variance parameter .

Data Valuation Method

Information theoretic measure of the quality of a trained model in terms of the reduction in uncertainty of model parameters. A higher quality model will have a higher value of information gain.

denoted by vector $\boldsymbol{\theta}$, after training on data D_C. We use the prior entropy $\mathbb{H}(\boldsymbol{\theta})$ and posterior entropy $\mathbb{H}(\boldsymbol{\theta}|D_C)$ to represent the uncertainty of $\boldsymbol{\theta}$ before and after training on D_C, respectively. So, if the data D_C for $C \subseteq N$ can induce a greater reduction in the uncertainty/entropy of $\boldsymbol{\theta}$ or, equivalently, *information gain* (IG) $\mathbb{I}(\boldsymbol{\theta}; D_C)$ on $\boldsymbol{\theta}$:

$$v_C \triangleq \mathbb{I}(\boldsymbol{\theta}; D_C) = \mathbb{H}(\boldsymbol{\theta}) - \mathbb{H}(\boldsymbol{\theta}|D_C)\,, \qquad (1)$$

Properties

- Data of an *empty* coalition has *no* value: $v_\emptyset = 0$.
- Data of any coalition $C \subseteq N$ has *non-negative* value: $\forall C \subseteq N \;\; v_C \geq 0$.
- **Monotonicity**. Adding more parties to a coalition cannot decrease the value of its data: $\forall C \subseteq C' \subseteq N \;\; v_{C'} \geq v_C$.
- **Submodularity**. Data of any party i is less valuable to a larger coalition which has more parties and data: $\forall i \in N \; \forall C \subseteq C' \subseteq N \backslash \{i\} \;\; v_{C' \cup \{i\}} - v_{C'} \leq v_{C \cup \{i\}} - v_C$.

The first 2 properties fulfill standard conditions of CGT. The latter 2 properties influence the model of reward scheme

Incentives - Definitions

R1 **Non-negativity.** $\forall i \in N \;\; r_i \geq 0$.

R2 **Feasibility.** The model reward received by each party in any coalition $C \in CS$ cannot be more valuable than the model trained on their aggregated data D_C: $\forall C \in CS \;\; \forall i \in C \;\; r_i \leq v_C$.

R3 **Weak Efficiency.** In each coalition $C \in CS$, the model reward received by at least a party $i \in C$ is as valuable as the model trained on the aggregated data D_C of C: $\forall C \in CS \;\; \exists i \in C \;\; r_i = v_C$.

R4 **Individual Rationality.** Each party should receive a model reward that is at least as valuable as the model trained on its own data: $\forall i \in N \;\; r_i \geq v_i$.

Fairness(R5)

Uselessness - $(\forall C \subseteq N \setminus \{i\} \;\; v_{C\cup\{i\}} = v_C) \Rightarrow r_i = 0\,.$

Symmetry - $(\forall C \subseteq N \setminus \{i,j\} \;\; v_{C\cup\{i\}} = v_{C\cup\{j\}}) \Rightarrow r_i = r_j\,.$

Strict Desirability - $(\exists B \subseteq N \setminus \{i,j\} \;\; v_{B\cup\{i\}} > v_{B\cup\{j\}}) \wedge$
$(\forall C \subseteq N \setminus \{i,j\} \;\; v_{C\cup\{i\}} \geq v_{C\cup\{j\}}) \Rightarrow r_i > r_j\,.$

Strict monotonicity - $(\exists B \subseteq N \setminus \{i\} \;\; v'_{B\cup\{i\}} > v_{B\cup\{i\}}) \wedge$
$(\forall C \subseteq N \setminus \{i\} \;\; v'_{C\cup\{i\}} \geq v_{C\cup\{i\}}) \wedge$
$(\forall A \subseteq N \setminus \{i\} \;\; v'_A = v_A) \wedge (v'_N > r_i) \Rightarrow r'_i > r_i\,.$

Shapley Value

$$\text{Shapley}_v(i) = \frac{1}{n!} \sum_{\pi \in \Pi_N} \left(v_{S_{\pi,i} \cup \{i\}} - v_{S_{\pi,i}} \right)$$

This valuation satishies R1,R2,R5 but to satisfy R4 and R3 we must scale it by some factor k. But due to submodularity of data, directly scaling by k may lead to violation of R4 still, hence we scale by a factor of k and exponentiate by some factor p. Also, intuitively reducing p reduces proportionality of r_i with $Ø_i$ hence the values of rewards come closer for parties with moderate/high difference of valuable data.

p-Shapley Fairness + Stability (R5)

Definition 2 (**ρ-Shapley Fairness**). *Given* $\{v_C\}_{C \in 2^N}$, *if there exist constants* $k > 0$ *and* $\rho > 0$ *s.t.* $r_i = k\phi_i^\rho$ *for all* $i \in N$, *then the values* $(r_i)_{i \in N}$ *of model rewards are* ρ*-Shapley fair.*

Stability :

Definition 3 (**Stability**). *A coalition structure* CS *with a given set* $(r_i)_{i \in N}$ *of values of model rewards is stable if* $\forall C \subseteq N \;\; \exists i \in C \;\; v_C \leq r_i$.

Conversely, supposing $\exists C \subseteq N \;\; \forall i \in C \;\; r_i < v_C$, all parties in C may be willing to deviate to form coalition C as they can feasibly increase the values of their model rewards (up) to v_C. The condition in Definition 3 is computationally

Definitions

R6 **Stability of Grand Coalition.** Suppose that the value of data is monotonic. The grand coalition is stable if for every coalition C, the value of the model reward received by the party with largest Shapley value is at least v_C:
$\forall C \subseteq N \;\; \forall i \in C \;\; \phi_i = \max_{j \in C} \phi_j \Rightarrow \; v_C \leq r_i \; .$

R7 **Group Welfare.** The values $(r_i)_{i \in N}$ of model rewards should maximize the group welfare $\sum_{i \in N} r_i$.

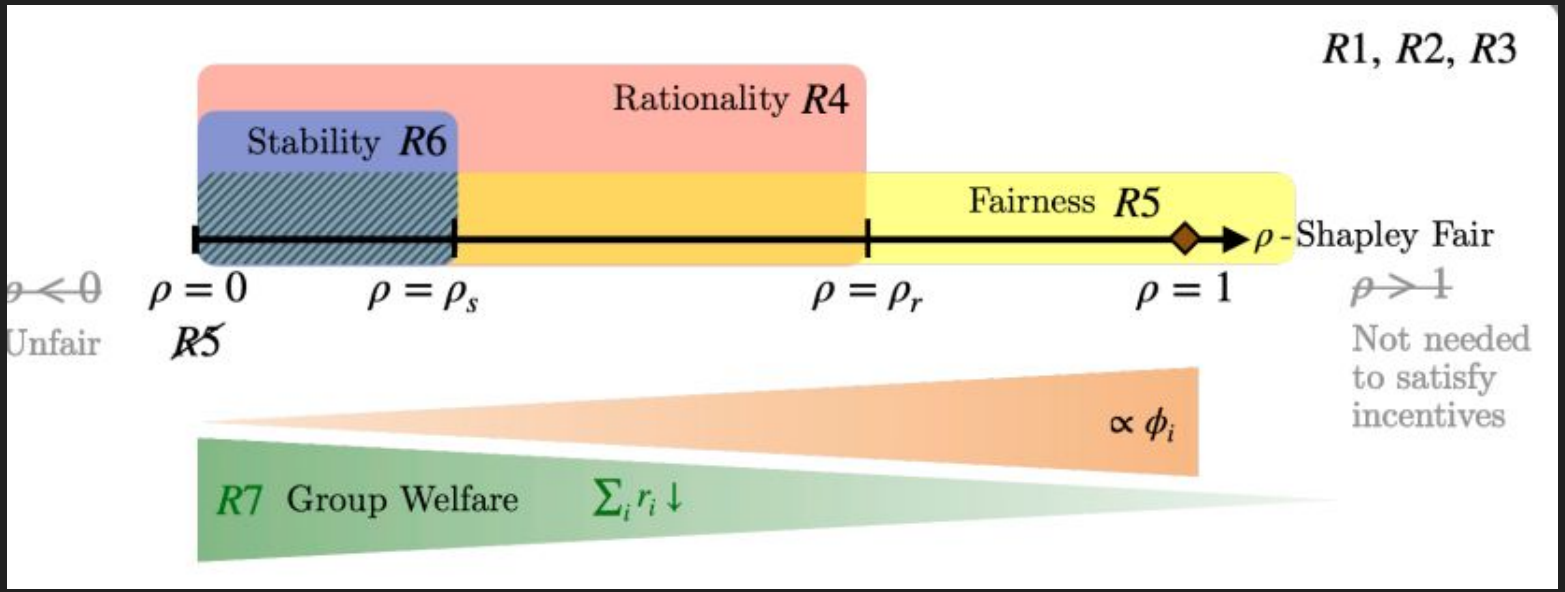
Reward Scheme Considering All Incentives

Theorem 1. *Let* $0 < \rho \leq 1$. *For each party* $i \in N$, *let* $\phi_i \triangleq \text{Shapley}_v(i)$ *and reward* $r_i \triangleq (\phi_i/\phi^*)^\rho \times v_N$ *where* $\phi^* = \max_{i \in N} \phi_i$.[8] *The values* $(r_i)_{i \in N}$ *of model rewards are* ρ*-Shapley fair and satisfy R1 to R3 and R5 when* $\rho > 0$. *Also, when*

- $\rho = 1$, $(r_i)_{i \in N}$ *are (pure) Shapley fair (Definition 1);*
- $\rho \leq \rho_r \triangleq \min_{i \in N} \log(v_i/v_N)/\log(\phi_i/\phi^*)$, $(r_i)_{i \in N}$ *satisfy individual rationality (R4);*
- $\rho \leq \rho_s \triangleq \min_{i \in N} \log(v_{C_i}/v_N)/\log(\phi_i/\phi^*)$ *where coalition* $C_i \triangleq \{j \in N \mid \phi_j \leq \phi_i\}$, $(r_i)_{i \in N}$ *achieve stability of the grand coalition (R6) and individual rationality (R4) as* $\rho_s \leq \rho_r$;
- $\rho = 0$, $(r_i)_{i \in N}$ *provide maximum group welfare (R7) but do not satisfy fairness (R5).*

Shapley constraints

In practice, the parties may agree to use a smaller p if they want to increase their total benefit from the collaboration or if they do not know their relative expected marginal contributions before hand



How rewards are distributed after collecting all data

We inject a gaussian noise function on the data aggravated from all other parties and vary the variance parameter from 0 to infinity to span all values of r_i. We use an efficient root finding algorithm to find the optimal variance parameter.

Advantages

Advantages

1. Introduces collaborative Machine Learning without monetary rewards.
2. Algorithm to calculate rewards is not computationally complex or costly.
3. Works well when no one party has enough information to make a highly predictive model and that is when collaboration usually takes place.

Disadvantages

1. High IG always does not correspond to a lower MNLP, although a weak relation exists.
2. A user cannot use the received rewards on a different type of kernel/learning algorithm and limits each party's flexibility to experiment with different model parameters and architectures.
3. The value of p to satisfy all conditions of rationality can be restrictive as distribution tends to be equal(slightly unfair) as we reduce the value of p to satisfy the conditions R6 and R4.
4. Cannot perform a different learning task on the same dataset as the reward is a trained model

Possible Improvements

1. We can explore the restrictions on p only when close competitors/market dominators collaborate as this is usually how markets run and this might reduce the submodularity of shapley function, thereby reducing restriction on p and hence finding bounds between highest and lowest valuation, incentivising a certain new entrant to reach a certain level to gain collaboration.