Optimized Data Sharing with Differential Privacy: A Game-theoretic Approach

Nan Wu, [*,‡], David Smith, [*,§], and Mohamed Ali Kaafar, [*,‡]

[‡]Macquarie University, [*]CSIRO's Data61, [§]Australian National University

System Model

There are several data owners training their own machine learning parameters with both their own dataset and other private datasets. They send queries to each other and respond with a randomised answer as in Figure 1. We extend the existing framework in [2] to multiple learners aiming to train their own ML models according to each others' separate privacy aware sub-gradient responses.

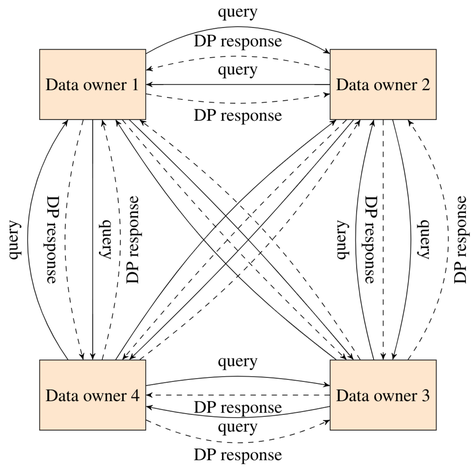

Figure 1: The communication structure between the distributed data owners (learners) for submitting queries and providing differentially-private (DP) responses to each other. The dashed lines are DP responses and solid lines are queries.

Contributions

- We evaluate the collaborative learning model with DP from a fixed-point view of linear regression contraction problem.
- We use a Banach fixed-point of view on gradients responses to modify the learning algorithm.
- We make a precise prediction of the learning parameter in ML model.
- We build a non-cooperative game model for these learners to optimally trade-off accuracy and privacy, according to privacy budget and gain with minimised learning loss.
- We demonstrate a unique Nash equilibrium for this game, providing a mutual best response in terms of the differentially private shared data and its learning loss.
- Our numerical tests demonstrate the significant benefits of learning using our game in privacy and social welfare with differentially-private collaborative machine learning.

Methods

We define the iteration problem in ML for linear regression model as a contraction problem from a fixed point of view on gradient methods [1]. Each agent has access to a set of private training data $\mathcal{D}_i := \{(x_i, y_i)\}_{i=1}^{n_i} \subseteq \mathbb{X} \times \mathbb{Y} \subseteq \mathbb{R}^{p_x} \times \mathbb{R}^{p_y}$, where x_i and y_i, respectively, denote inputs and outputs.

In linear regression, the loss function is to minimize the following Mean Square Error $f(\theta)$:

$$f(\theta) = \|\theta X' - Y'\|_2^2$$

The operation of the fixed point iterations problem is defined as $\mathcal{T}^\rho : \mathbb{R}^n : \mathbb{R} : \theta \to \mathcal{T}(\theta)$

$$\mathcal{T}(\theta_i[k+1]) = \theta_i[k] - \frac{\rho_k}{n_\ell}\left[\frac{2}{n_i}(\theta_i[k]X_i' - Y_i')X_i + Q_i[k]\right] \tag{1}$$

where $Q_i[k]$ is the received query responses from all other data owners at iteration k.

The learning parameter θ_{k+1} for next iteration can be predicted by current and previous learning parameter θ_{k-1} and θ_k:

$$\theta_{k+1} = \theta_k + (\theta_k - \theta_{k-1})(\mathbb{I} - \frac{2\rho}{n_\ell}X_\ell' X_\ell - \frac{2\rho}{n_\ell}\sum_{j\in\mathcal{N}\setminus\{i\}} n_j \mathbb{E}(w(j;k;\epsilon_j))) \tag{2}$$

Game Model

The game G is finitely repeated $T < \infty$ times, with imperfect information.

- A dynamic noncooperative repeated game $G = [\mathcal{N}, \epsilon_\mathbf{i}, J_{i,\tau}(\cdot)]$ at each time stage τ of gameplay.
- $n = 1, ..., N$ are the player/data-owners in $\mathcal{N}$.
- $\boldsymbol{\epsilon_i} = [0.1, 10]$ is the (pure) strategy set for the ith data owner.
- The space of action profiles for the N players in each stage is $\boldsymbol{\epsilon} = \epsilon_1 \times \epsilon_2 \times, \ldots \epsilon_N$.
- The cost function for data owner i is

$$J_i(\epsilon_i, \epsilon_{-i}) = c_i(\epsilon_i) + f(\epsilon_i) \tag{3}$$

where c_i is referred as disclosure cost, which is thus non-negative continuous decreasing [3], $f(\epsilon_i)$ is non-negative continuous and increasing learning loss prediction obtained from equation (2).

A Unique Nash Equilibrium can be reached.

Results

We use a lending dataset with a linear regression model to demonstrate the value of the methodology and to validate the theoretical results. The **inputs** contain loan attributes, such as total loan size, and borrower information, such as number of credit lines, state of residence, and age. The **outputs** are the interest rates of the loans per annum.

Learning Parameter Prediction

The performance of the learning parameter prediction is shown as learning loss in Mean Square Error (MSE), versus privacy budget value in Figure 2.

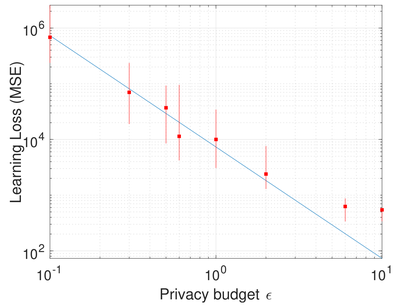

Figure 2: Statistic of Learning loss (MSE) versus privacy budget ϵ. The solid blue line is the prediction of the learning loss value by fixed point contraction method

Collaborative learning with game theory

Game helps in choosing the best response of privacy budget value for all players as shown in Table 1.

Number of players	3 players	4 players	5 players
SC(with game)	1.3230	1.2060	0.5640
RMSE(with game)	$2.62\epsilon^2$	$1.70\epsilon^2$	83.6
Average ϵ	0.6433	0.5250	0.3160
SC(without game)	0.03	0.04	0.05
RMSE(without game)	$1.60\epsilon^3$	$8.26\epsilon^2$	$4.87\epsilon^2$
ϵ for all players	0.1	0.1	0.1
SC(without game)	2.3234	2.7233	3.5824
RMSE(without game)	$1.85\epsilon^2$	$1.00\epsilon^2$	55.4
ϵ for all players	1	1	1
SC(without game)	3.3446	4.8803	4.9494
RMSE(without game)	23.33	18.42	24.02
ϵ for all players	10	10	10

Table 1: Social Cost (SC) and Learning Loss(RMSE) for different players with and without game

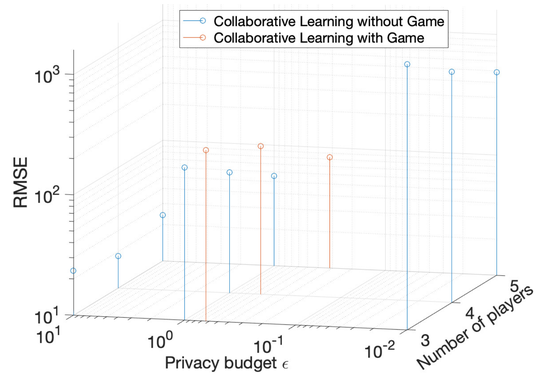

Figure 3: Learning loss (RMSE) versus privacy budget ϵ for 3, 4, and 5 data owners in collaborative learning with and without game

The average learning loss with $\epsilon = 10$ for all data owners is the lowest in Figure 3. With the increase of the DP noise magnitude, the average learning loss increases non-linearly. The Equilibrium result between the learning loss and privacy budget ϵ is shown in red plots in this figure. **There is a significant improvement in privacy, which is about 47.5%.**

Social Welfare

We define the social cost per player: $SC = \frac{1}{\mathbb{N}}\sum_{i\in\mathbb{N}} J_i(\epsilon_{i,k=T})$.

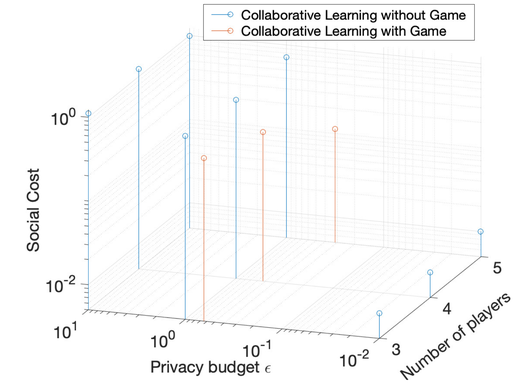

Figure 4: Social cost (SC) versus privacy budget ϵ for 3, 4, and 5 data owners in collaborative learning with and without game

The social cost for collaborative learning with game is lower in the case when $\epsilon = 1$ with any number of players in Figure 4. The learning loss and privacy budget not only reaches a balance at the equilibrium but also **minimises the social cost per player**.

References

[1] Alexander Jung. A fixed-point of view on gradient methods for big data. *Frontiers in Applied Mathematics and Statistics*, 3:18, 2017.

[2] N. Wu, F. Farokhi, D. Smith, and M. Kaafar. The value of collaboration in convex machine learning with differential privacy. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 485–498, Los Alamitos, CA, USA, may 2020. IEEE Computer Society.

[3] Tao Zhang and Quanyan Zhu. Dynamic differential privacy for ADMM-based distributed classification learning. *IEEE Transactions on Information Forensics and Security*, 12(1):172–187, 2017.