Notation and Conventions

General

- If $f = g + h$ and g is differentiable but h is non-differentiable, overload the ∇ operator by defining $\nabla f \coloneqq \nabla g$.
- $\|\cdot\|$: Euclidean norm
- $\angle(v, w)$: the angle between vectors v and w

Non-Federated Sparse Linear Regression

- (X, Y): training dataset
- λ: L1 regularization parameter
- β: model
- $f(\beta) \coloneqq f(X, Y, \lambda, \beta)$: objective function of sparse linear regression
- $\beta^* \coloneqq \arg\min_\beta f(\beta)$: optimal model
- β^s: model at s-th iteration
- η: step-size
- $S_{\lambda\eta}(\cdot)$: soft-thresholding operator

Federated Sparse Linear Regression

- K: number of clients
- G: communication graph
- $\mathrm{ne}(i)$: neighborhood of i-th client
- $K_i \coloneqq 1 + |\mathrm{ne}(i)|$: the number of neighbors of the i-th client including itself
- Let the index i range over $\{1, \ldots, K\}$, and the index j range over $\{i\} \cup \mathrm{ne}(i)$.
- (X_i, Y_i): i-th private training dataset
- $(X, Y) \coloneqq \bigcup_i (X_i, Y_i)$: joint training dataset
- $f_i(\beta) \coloneqq f(X_i, Y_i, \lambda, \beta)$: i-th objective function
- β_i: i-th local model

1 Problem Statement

The most basic problem is "sparse linear regression", which is well understood. This problem is generalized by "federated sparse linear regression", which is in turn generalized by the main problem, "federated sparse linear regression with poisoning attacks".

1.1 (Non-Federated) Sparse Linear Regression

The most basic setting is the non-federated setting, in which a single client possesses a training dataset (X, Y) and wants to find an optimal model $\beta^* := \arg\min_\beta f(X, Y, \lambda, \beta)$. For conciseness we can suppress X and Y and simply write the objective function as $f(\beta)$. The objective function $f(\beta)$ is the objective function for sparse linear regression.

1.2 Federated Sparse Linear Regression

More generally, in the federated setting there are K clients, each possessing a private training dataset (X_i, Y_i). Define the joint training dataset $(X, Y) = \bigcup_i (X_i, Y_i)$. The clients want to find an optimal model $\beta^* = \arg\min_\beta f(\beta)$ (the objective function depends on the joint training dataset). To collaborate, the clients broadcast messages to their neighbors on a graph G. These messages must not include private training datasets, but can include models and gradients.

1.3 Federated Sparse Linear Regression with Poisoning Attacks

Even more generally, assume that all clients are either benign or adversarial. Benign clients want to recover the optimal model as before, but adversaries will intentionally broadcast incorrect models and/or gradients to their neighbors in order to prevent convergence.

2 Methods

Sparse linear regression is solved by "proximal gradient descent". We examine how this method can be generalized to "federated sparse linear regression", and generalized again to "federated sparse linear regression robust to poisoning attacks".

2.1 Proximal Gradient Descent

All algorithms to follow will generalize proximal gradient descent, which solves non-federated sparse linear regression and has the following steps:

Gradient (G): $\beta_i \leftarrow \beta_i - \eta \nabla f_i(\beta_i)$.

Threshold (T): $\beta_i \leftarrow S_{\lambda\eta}(\beta_i)$.

2.2 Federated Proximal Gradient Descent

The first generalization of proximal gradient descent is to the federated setting. A federated method must include an aggregation step:

Consensus (C): $\beta_i \leftarrow \beta_i + \frac{\eta}{K_i}\sum(\beta_j - \beta_i)$

Aggregate (A): $\beta_i \leftarrow \beta_i - \frac{\eta}{K_i}\sum \nabla f_j(\beta_j)$

Aggregate Plus (A+): $\beta_i \leftarrow \beta_i - \frac{\eta}{K_i}\sum \nabla f_j(\beta_i)$.

Aggregation steps can be performed one after the other (sequentially) or at the same time (simultaneously). For now we will ignore simultaneous aggregation steps involving A+.

(AC): $\beta_i \leftarrow \beta_i - \frac{\eta}{2K_i}\sum (\nabla f_j(\beta_j) - (\beta_j - \beta_i))$

(GC): $\beta_i \leftarrow \beta_i - \frac{\eta}{2K_i}(K_i\nabla f_i(\beta_i) - \sum(\beta_j - \beta_i))$.

To enable aggregation steps, we also require broadcasting steps. All aggregation steps except for A+ require a single broadcast (B). A+ actually requires two rounds of broadcasting (B+).

Broadcast (B): $i \xrightarrow{m\subseteq\{\beta_i, \nabla f_i(\beta_i)\}} j$

Broadcast Plus (B+): $i \xrightarrow{\{\beta_i\}} j \xrightarrow{\{\nabla f_j(\beta_i)\}} i$

We have an alphabet of G, T, C, A, A+, (AC), (GC), B, and B+. The letters G, C, A, A+, (AC), and (GC) are "aggregation steps" (think of G as a degenerate case) and the letters B and B+ are "broadcasting steps". All of the methods for federated proximal gradient descent are strings consisting of letters of the alphabet. We need grammatical rules determining which strings are "well-formed". These rules will yield a list of methods worth investigating, and will be informed by common sense assumptions.

Assumption: Output must be sparse.

1. T occurs exactly once and occurs last.

Assumption: No more gradients than necessary.

2. A+ is banned.
3. Exactly one of A and G occurs.

Assumption: No more broadcast rounds than necessary.

4. If A or C occurs, then B occurs exactly once and occurs directly before the earliest A or C.

5. C occurs at most once.

   Assumption: Don't use information that is out of date.

6. AC and CA are banned.

Thus, the complete list of methods: G, A, (AC), CG, GC, (GC).

Name	Rule	Cost	"Informativeness"
G	$\beta_i \leftarrow \beta_i - \eta \nabla f_i(\beta_i)$	Low	Low
C	$\beta_i \leftarrow \beta_i + \frac{\eta}{K_i} \sum (\beta_j - \beta_i)$	Medium	Medium
A	$\beta_i \leftarrow \beta_i - \frac{\eta}{K_i} \sum \nabla f_j(\beta_j)$	Medium	Medium
A+	$\beta_i \leftarrow \beta_i - \frac{\eta}{K_i} \sum \nabla f_j(\beta_i)$	High	High

2.3 Federated Proximal Gradient Descent Robust to Poisoning Attacks

We use a two step process to make our method robust to poisoning attacks. First, at each iteration, for each client i, and each of its neighbors j, client i receives the message $m \subseteq \{\beta_j, \nabla f_j(\beta_j)\}$, and computes a **model-based similarity measure** based on β_i and β_j, and/or a **gradient-based similarity measure** based on $\nabla f_i(\beta_j)$ and $\nabla f_j(\beta_j)$. Low similarity indicates suspicious behavior during an iteration. Second, client i computes a **trust score** for client j based on the history of similarity scores between clients i and j. Aggregation is now a weighted sum, and the j-th term is appropriately magnified or downweighed based on the j-th similarity score.

2.3.1 Similarity Measures

The formula for a similarity measure is informed by geometry. The models β_i and β_j are points, and the gradients $\nabla f_i(\beta_j)$ and $\nabla f_j(\beta_j)$ are arrows emanating from β_j. For models, we check whether they are getting closer over time:

$$\|\beta_i^s - \beta_j^s\| < \|\beta_i^{s-1} - \beta_j^{s-1}\|.$$

For gradients, we check the size of the angle between them:

$$\cos(\angle(\nabla f_i(\beta), \nabla f_j(\beta))).$$

The set of similarity measures available is dependent on the scheme.

Argument	Rule	Use Case
Models	$\|\beta_i^s - \beta_j^s\| < \|\beta_i^{s-1} - \beta_j^{s-1}\|$	C
Gradients	$\cos(\angle(\nabla f_i(\beta_j), \nabla f_j(\beta_j)))$	A
Gradients	$\cos(\angle(\nabla f_i(\beta_i), \nabla f_j(\beta_i)))$	A+

2.3.2 Trust Scores

3 The Written Qualifying Exam

WRITE ABOUT HOW THE WQE FITS INTO THIS FRAMEWORK