Federated Learning

Announcements

° No class next week
  ➔ Also no office hours

° I assume everyone has submitted project updates
  ➔ Responded to some, will get to others soon
- Need/Desire for Data Privacy

- Differential Privacy: How to Reveal the Output of a function computed on private data without leaking the private data: Reveal $F(x)$ without revealing $x$.

- Today: How to compute $F(x)$ without revealing $x$.

Computing $F(x)$ without revealing $x$:

- Core Techniques
  - L: Compute on encrypted data
  - General (3) Computation
    - Homomorphic Encryption/FHE
    - Multi-Party Computation

ML only? $\xrightarrow{3} \text{Federated Learning}$ Communication/Coordination

Federated Learning

Minimize power consumption + Compute f.Net
Challenges?

Stragglers

Straggler causes do:
\[ U = \text{hash}(\text{in}) \]

* All tasks start
* Red. process
  * L2 OS
  * L2 OS

* Garbage Collector
* Net Conviction
  * Processors difference - DC?
* Some other process
  * Running - Noisy

* Fail to complete
Applying this to Federated Learning

1. Procedure differences
2. Bottlenose
3. Cellphone resource

$\Rightarrow M \frac{(d_i-T)}{e}$
How To Choose Replicas

- Fairness

...
Federated Learning: Optimizing Performance

- Uniform compute devices + GPU
- Synchronize rounds based on...
- Build in UX for feedback
- Store and delay - Efficiencies

Is Fed Learning only for privacy?
Optimal Conditions for Federated Learning

Cost of Decentralization
Overview of Homomorphic Encryption, MultiParty Computation