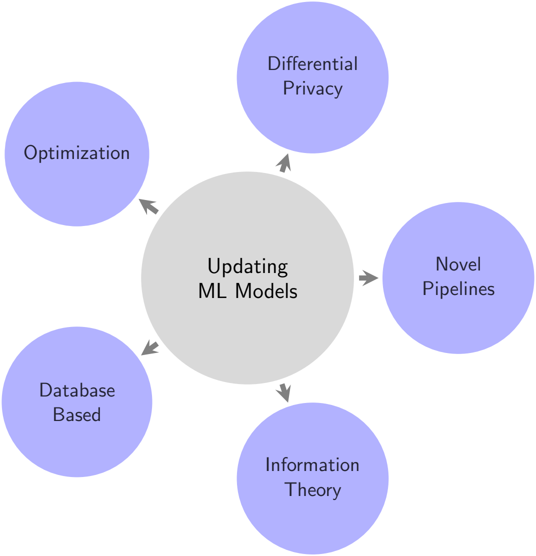
Updating ML Models

Ananth Mahadevan

November 7, 2020

Overview

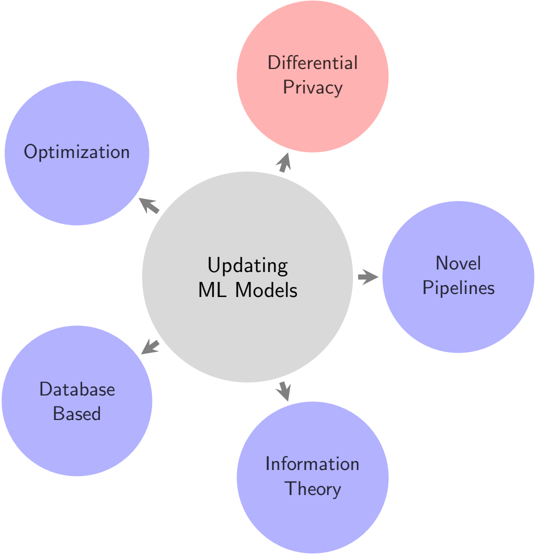
1. Motivation
2. Problem Overview
3. Approaches
    - Differential Privacy
    - Optimization
    - Database Based
    - Information Theory
    - Novel Pipelines
4. Next Directions


Updating
ML Models
Optimization
Differential
Privacy
Novel
Pipelines
Database
Based
Information
Theory

Common Terminology

- Fixed training Dataset $\mathcal{D}$
- Learning Algorithm A (can be randomized)
- Datapoints to be remove $\mathcal{D}_{\mathcal{R}}$, where $|\mathcal{D}_{\mathcal{R}}| = r$, remaining dataset $\mathcal{D}' = \mathcal{D} - \mathcal{D}_{\mathcal{R}}$
- Naive approach is retraining from scratch, i.e, $A(\mathcal{D}')$
- Mechanism M which offers an efficient way to update the model

Differential Privacy



Certified Data Removal [Guo et al., 2020]

Optimization

- Hello

References I

Guo, C., Goldstein, T., Hannun, A., and van der Maaten, L. (2020).
Certified Data Removal from Machine Learning Models.
arXiv:1911.03030 [cs, stat].