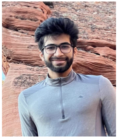
Private optimization in the interpolation regime: faster rates and hardness results


Hilal Asi*


Karan Chadha*

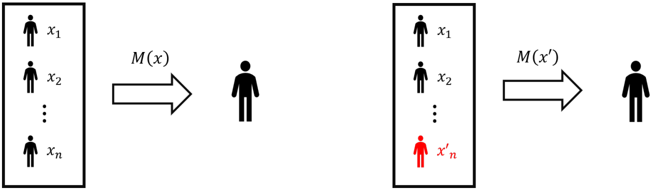

Gary Cheng*


John Duchi

Stanford University

ICML 2022

Differential Privacy Definition



- A mechanism M is (ε, δ)-*differentially private* if for every set S and for every pair of datasets x, x' differing by one entry

$$\mathbb{P}\left(M(x) \in S\right) \leq e^{\varepsilon} \mathbb{P}\left(M(x') \in S\right) + \delta.$$

Differentially Private Stochastic Convex Optimization

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x;S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

- $F(\cdot; s)$ is a convex loss function, L-Lipschitz and H-smooth
- $\mathcal{X} \subset \mathbb{R}^d$ is the parameter space (diameter D)

Differentially Private Stochastic Convex Optimization

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x; S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

- $F(\cdot; s)$ is a convex loss function, L-Lipschitz and H-smooth
- $\mathcal{X} \subset \mathbb{R}^d$ is the parameter space (diameter D)

A lot of work studying SCO & DP-SCO [Bassily et al. 20, Feldman et al. 21]

Differentially Private Stochastic Convex Optimization

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x;S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

- $F(\cdot; s)$ is a convex loss function, L-Lipschitz and H-smooth
- $\mathcal{X} \subset \mathbb{R}^d$ is the parameter space (diameter D)

A lot of work studying SCO & DP-SCO [Bassily et al. 20, Feldman et al. 21]

- Optimal rates without privacy $O\left(\frac{LD}{\sqrt{n}}\right)$

Differentially Private Stochastic Convex Optimization

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x; S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

- $F(\cdot; s)$ is a convex loss function, L-Lipschitz and H-smooth
- $\mathcal{X} \subset \mathbb{R}^d$ is the parameter space (diameter D)

A lot of work studying SCO & DP-SCO [Bassily et al. 20, Feldman et al. 21]

- Optimal rates without privacy $O\left(\frac{LD}{\sqrt{n}}\right)$
- Optimal rates with privacy $LD \cdot O\left(\frac{1}{\sqrt{n}} + \frac{d}{n\varepsilon}\right)$ [Feldman et al. 20, Asi et al. 21]

Differentially Private Stochastic Convex Optimization

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x;S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

- $F(\cdot; s)$ is a convex loss function, L-Lipschitz and H-smooth
- $\mathcal{X} \subset \mathbb{R}^d$ is the parameter space (diameter D)

A lot of work studying SCO & DP-SCO [Bassily et al. 20, Feldman et al. 21]

- Optimal rates without privacy $O\left(\frac{LD}{\sqrt{n}}\right)$
- Optimal rates with privacy $LD \cdot O\left(\frac{1}{\sqrt{n}} + \frac{d}{n\varepsilon}\right)$ [Feldman et al. 20, Asi et al. 21]

Privacy comes at a price in SCO!

Can we identify problems where we can get faster rates?

Can we identify problems where we can get faster rates?

We consider Interpolation Problems: problems where sample functions share a common minimizer.

Can we identify problems where we can get faster rates?

We consider Interpolation Problems: problems where sample functions share a common minimizer.

Definition (Interpolation Problem)

An interpolation problem is one where there exists $x^\star$ such that $\nabla F(x^\star; s_i) = 0$ for all $i \in [n]$.

Problem statement summary

Given $S_1^n \stackrel{\text{iid}}{\sim} P$, develop private algorithms that solve

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x; S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

Problem statement summary

Given $S_1^n \stackrel{\text{iid}}{\sim} P$, develop private algorithms that solve

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x;S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

Non-private optimization: rates of convergence improve from $\frac{1}{\sqrt{n}}$ to $\frac{1}{n}$

Problem statement summary

Given $S_1^n \stackrel{\text{iid}}{\sim} P$, develop private algorithms that solve

$$\begin{aligned} &\text{minimize} \;\; f(x) = \mathbb{E}_P[F(x; S)] \\ &\text{subject to} \;\; x \in \mathcal{X} \end{aligned}$$

Non-private optimization: rates of convergence improve from $\frac{1}{\sqrt{n}}$ to $\frac{1}{n}$

Similar improvments in private optimization?

Contributions

1. Interpolation does not help without additional assumptions
   - Cannot improve privacy cost in general

Contributions

1. Interpolation does not help without additional assumptions
   - Cannot improve privacy cost in general
2. Faster rates under quadratic growth

Contributions

1. Interpolation does not help without additional assumptions
   - Cannot improve privacy cost in general
2. Faster rates under quadratic growth
   - Sample size to achieve error α:

Non-interpolation: $\frac{d}{\varepsilon\sqrt{\alpha}}$ Interpolation: $\sim \frac{1}{\alpha^{\rho}} + \frac{d}{\rho\varepsilon}\log\left(\frac{1}{\alpha}\right)$

Contributions

1. Interpolation does not help without additional assumptions
   - Cannot improve privacy cost in general
2. Faster rates under quadratic growth
   - Sample size to achieve error α:

     Non-interpolation: $\frac{d}{\varepsilon\sqrt{\alpha}}$ Interpolation: $\sim \frac{1}{\alpha^\rho} + \frac{d}{\rho\varepsilon}\log\left(\frac{1}{\alpha}\right)$
3. Algorithms that adapt to interpolation
   - Achieve faster rates for interpolation problems while retaining optimal rates for non-interpolation problems

Contributions

1. Interpolation does not help without additional assumptions
   - Cannot improve privacy cost in general
2. Faster rates under quadratic growth
   - Sample size to achieve error α:

     Non-interpolation: $\frac{d}{\varepsilon\sqrt{\alpha}}$ Interpolation: $\sim \frac{1}{\alpha^\rho} + \frac{d}{\rho\varepsilon}\log\left(\frac{1}{\alpha}\right)$
3. Algorithms that adapt to interpolation
   - Achieve faster rates for interpolation problems while retaining optimal rates for non-interpolation problems
4. Optimality and the price of adaptivity

Please visit our poster #1011 tonight to learn more!

Please visit our poster #1011 tonight to learn more!

Thank you!