Differentially Private Stochastic Coordinate Descent

Georgios Damaskinos, Celestine Dunner,
Rachid Guerraoui, Nikolaos Papandreou, Thomas Parnell

PPML @ NeurIPS 2020

Problem

SCD is **popular** in both Academia and Industry

- 154 research articles with "coordinate descent" in the title since 2019
- Default solver for *Scikit-Learn, TensorFlow, Liblinear, IBM Snap-ML*

Why so popular ?

✓ Low tuning cost (no learning rate)
✓ Often favorable convergence guarantees
➢ In particular for GLMs

SCD applications involve **sensitive data**

- healthcare
- finance
- social media

...

> *Can SCD maintain its **benefits** alongside **strong privacy** guarantees ?*

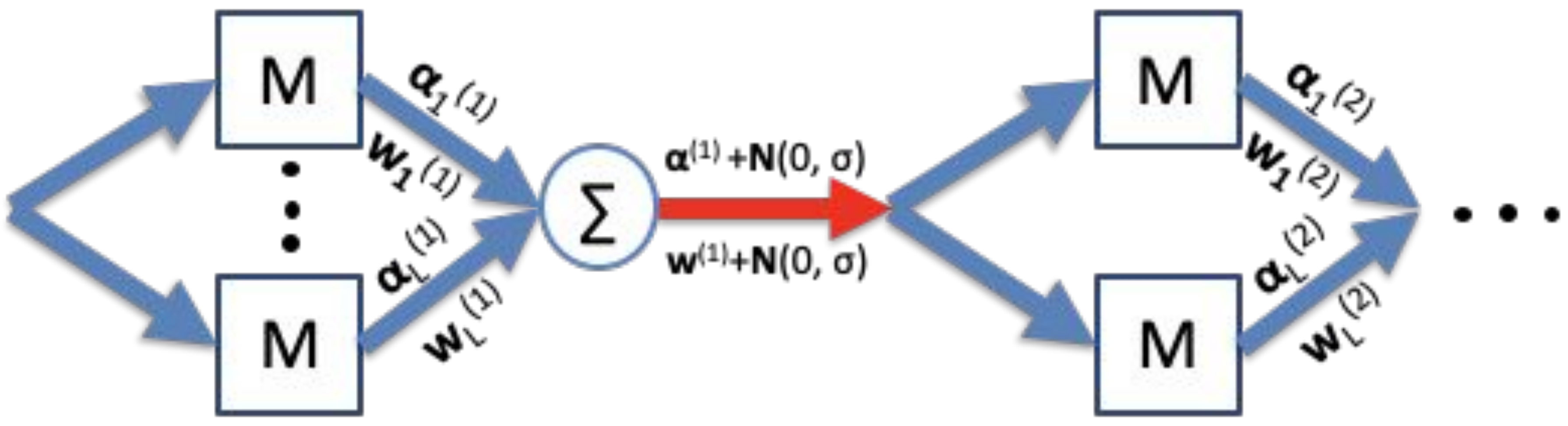
DP-SCD

Challenge

Differential privacy requires *independent* noise addition to **α** and **w**
=> No consistency: **w** ≠ $\mathbf{X}^T \cdot \boldsymbol{\alpha}$

1. Convergence guarantees ?
2. Competitive privacy-utility trade-off ?

Design



- Parallel updates (mini-batch)
- Update scaling

Notation

X	Input dataset ($\mathbb{R}^{m \times n}$)
w	Shared vector
α	Dual vector
N(0, σ)	Gaussian noise
ε	Privacy loss bound
C	Scaling factor
M	Coordinate update mechanism

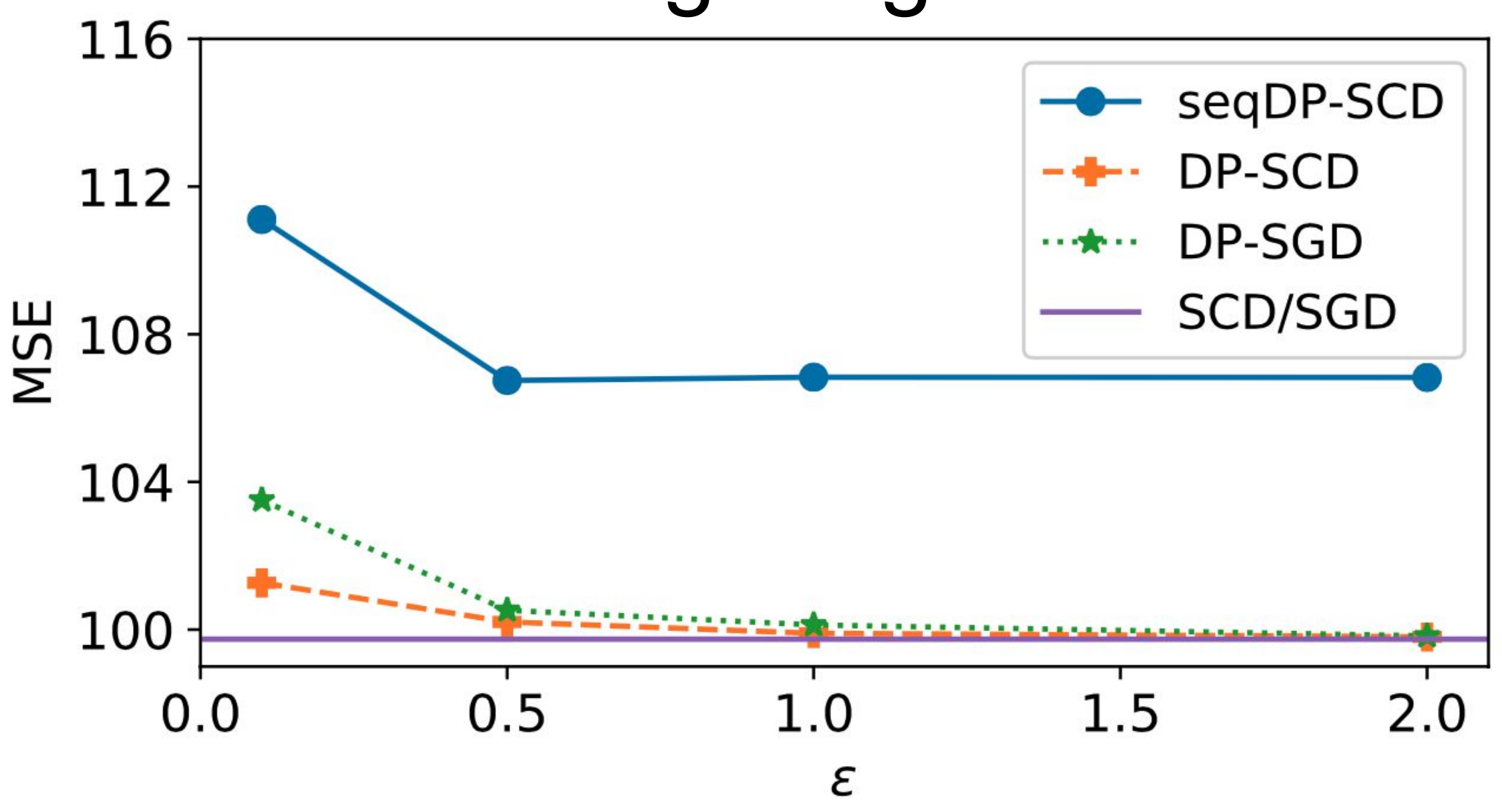
Convergence

Consistency *holds in expectation*

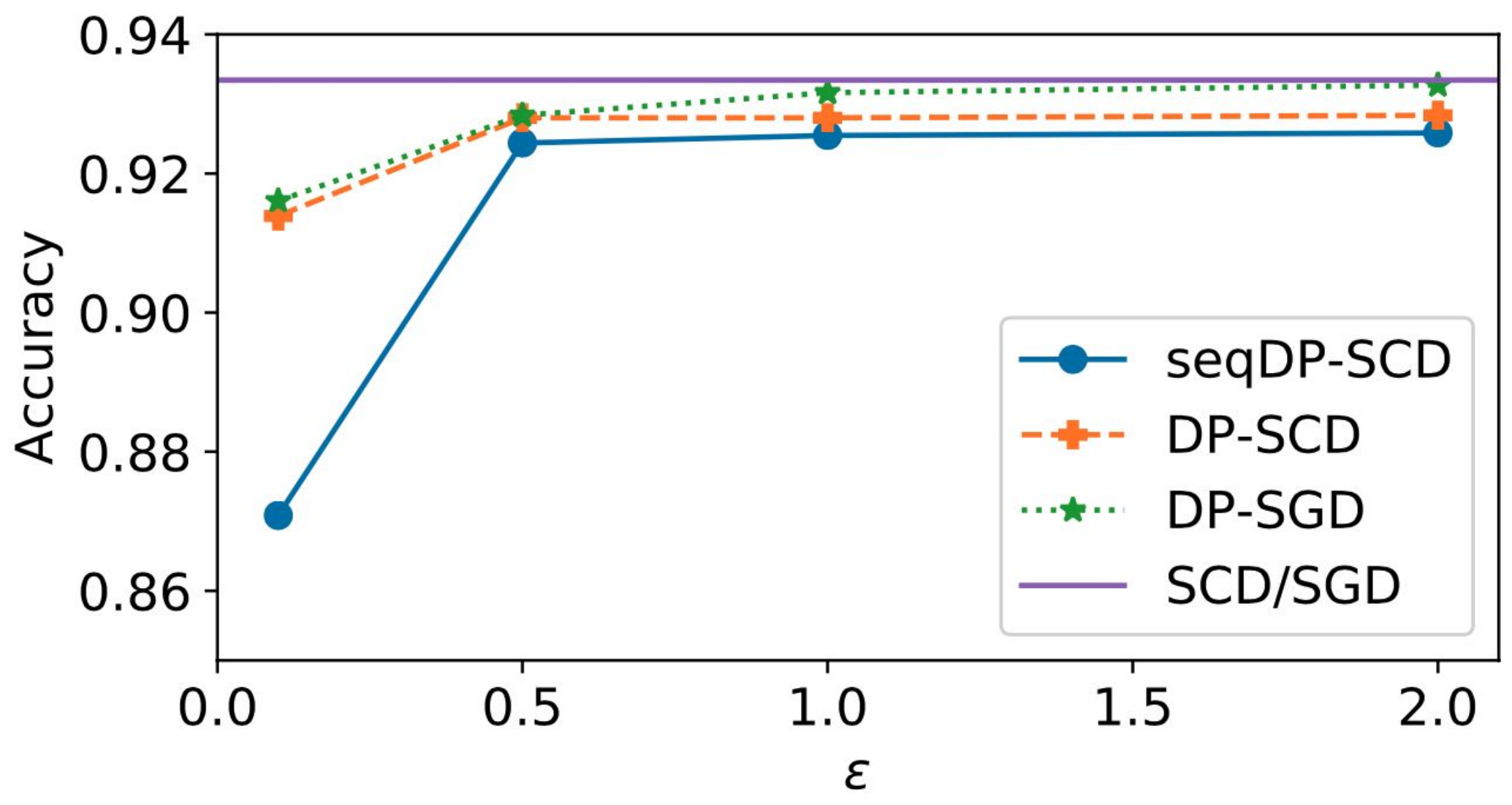
Method	Perturbation	Utility Bound
(Zhang et al. 2017)	Output	$\mathcal{O}\left(\frac{m}{n^2\epsilon^2}\right)$
(Chaudhuri and Monteleoni 2009) (Chaudhuri, Monteleoni, and Sarwate 2011)	Inner (objective)	$\mathcal{O}\left(\frac{m}{n^2\epsilon^2}\right)$
(Wang, Ye, and Xu 2017)	Inner (update)	$\mathcal{O}\left(\frac{m\cdot\log(n)}{n^2\epsilon^2}\right)$
DP-SCD	Inner (update)	$\mathcal{O}\left(\frac{L^3\cdot\log(\frac{n}{L})}{n^4\epsilon^2}\right)$

Evaluation

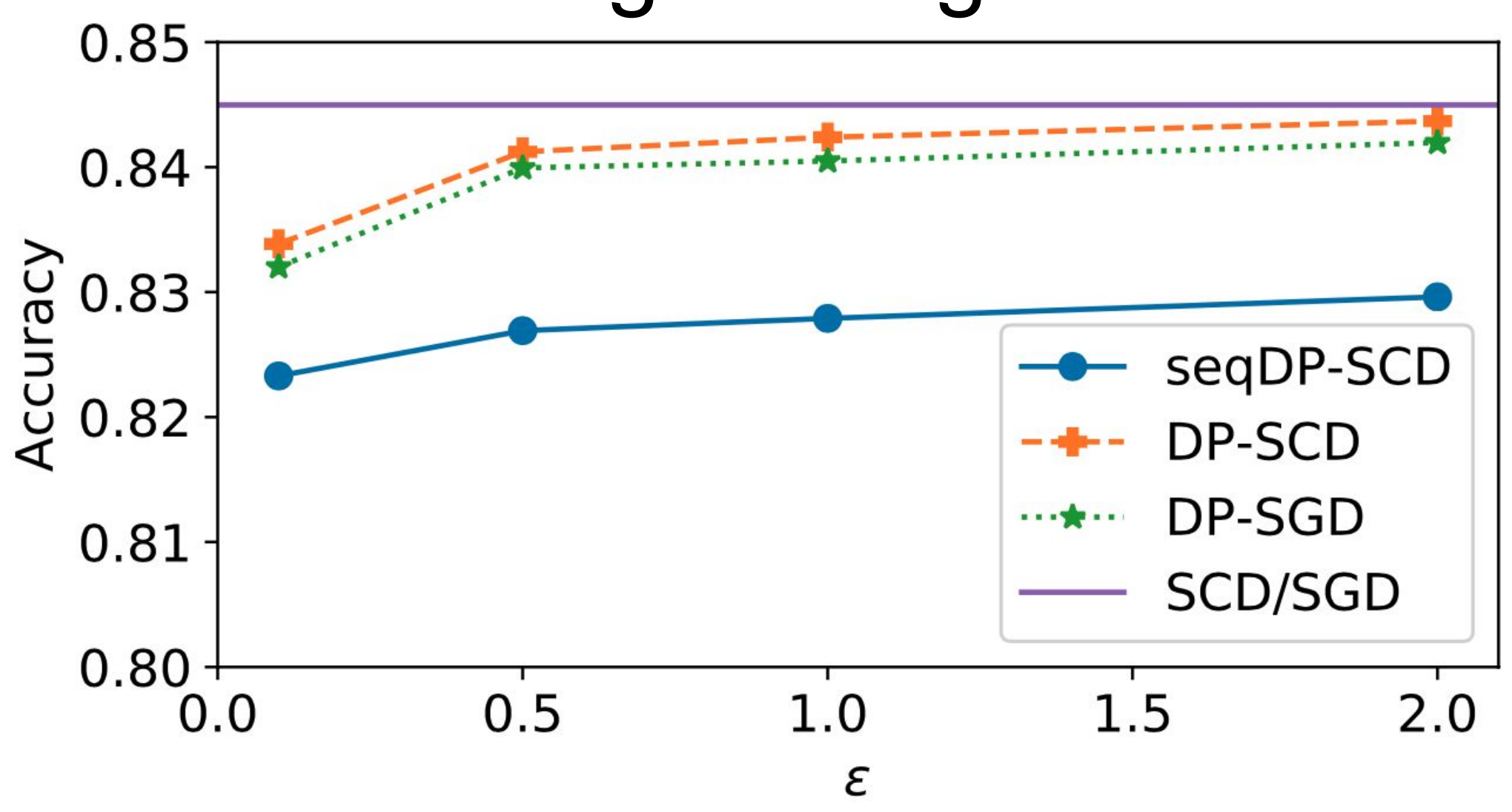
Ridge regression



SVMs

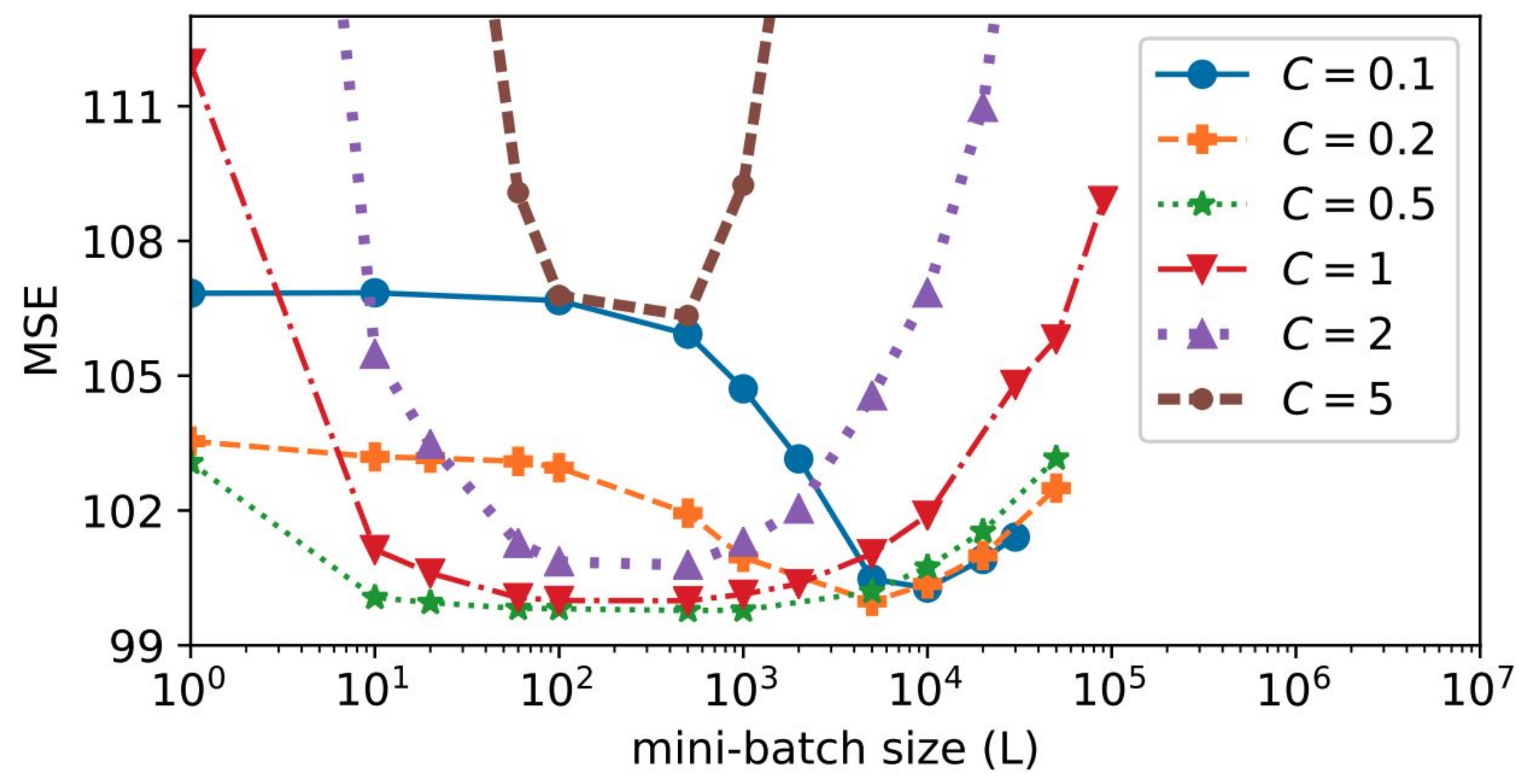


Logistic regression



DP-SCD outperforms DP-SGD for the applications that enable exact update steps (ridge regression and SVMs)

parallelism - scaling interplay



Deviating from the best choice for C (C = 0.5 for this setup), reduces the width of the flat area and moves the minimum to the right (for smaller C values) or upwards (for larger C values)

https://github.com/gdamaskinos/dpscd

contact: georgios.damaskinos@gmail.com