Differentially private modification of sign-SGD

Alexey Kravatskiy

Moscow Institute of Physics and Technology

Course: My first scientific paper
(Strijov's practice)/Group 205

Expert: A. N. Beznosikov

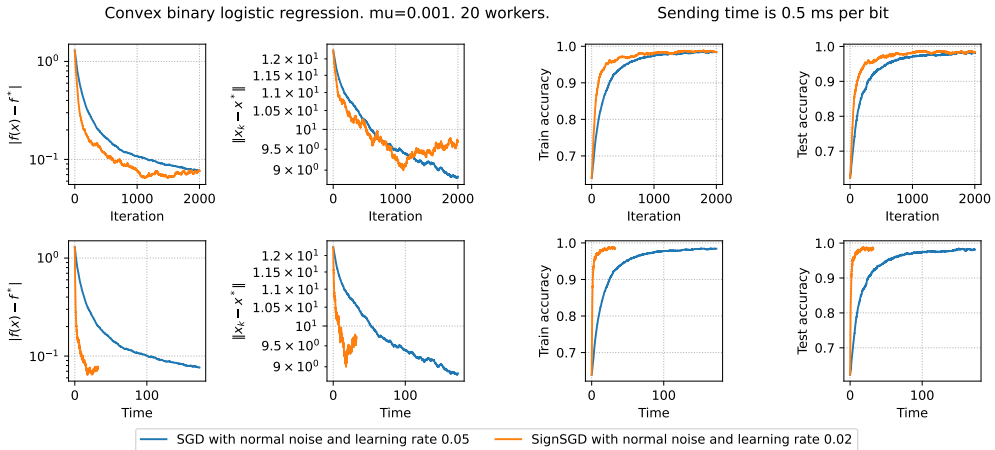
Consultant: S. A. Chezhegov

2025

Goal of research

One-slide talk

Please comment all slides but this one if you make the One-slide talk.



Column 2

Column 1

The message.

Literature

Differential Privacy

Renyi differential privacy

Criterion of a private algorithm

Sample Gaussian Mechanism

Solution

Column 1

Column 2

Computational experiment

Conclusion

dp-sign SGD

- with Poisson sampling $q = 1/n$
- is $(10, 1/n^{1}.1)$ private
- empirically converges on logistic regression problem

Now we have to provide theoretical guarantees of convergence.