Differential Privacy for Machine Learning

Master IASD, Université PSL

February 2023

Project Guidelines

The project for this year takes the form of a critical analysis of an article, the reproduction of its experiments and their application to other datasets.

- By a group of 3 members, you must indicate your top 3 choices from the list of 11 papers below. Each group will have 5 points to allocate to the list of papers. You can only allocate integer bids to each paper. Here are some example bids.
- The organization of the work in the group should be balanced. It is your responsibility to decompose the work equitably.
- Each member should be able to state clearly which part the work he was in charge of.
- If you are absolutely unable to form a group of 3 members, you may form a group of 2 members. But, we highly recommend a group of size 3.

Project Report

The report should be organized as follows:

- An introduction to the problem: why it is relevant, to which question it answers
- The state of the art of the subject tackled by the paper. Go beyond the papers cited in the article.
- The main results of the paper; how they advance the state of the art
- A critical analysis of the merits and limitations of the proposed approach
- A replication of the experiments
- Your contribution on top of the paper's results.
- A conclusion with an emphasis on open questions

Project Report

Ideas for your contribution:

- A slight modification to the main algorithms. You can try multiple modifications and explain in your report what worked, what did not and why.
- Applying the technique/algorithms to new setting (new dataset, or new task, or a slightly different objective).
- If possible, a simple extension to the theoretical results of the paper (for example, stronger results with more stringent assumptions, or more general result with weakened assumptions).

Project Report

- **Format:** The report should be formatted following the Latex template of the ICML conference at this link, with $6 - 8$ pages not counting references.
- **Evaluation:** You will be evaluated on clarity of the analysis of the chosen article, the rigor and the extensive character of the analysis and/or the experiments carried out, and expression, clarity of explanation and quality of exposition.
- **Code:** When possible, you can provide a companion code in the form of a Jupyter notebook, preferably by providing a link to a Colab notebook.

Project Presentation

You will have 15 min for presenting your work. The presentation can be structured as follows.

- 2 min: introduction of the problem, its motivation, and its relevance
- 3 min: presentation of prior work
- 5 min: presentation of the main results and their scope
- 5 min: critical analysis and open problems

The presentation will be followed by up to 15 min of questions.

Important dates

- By March 3, 23:00 Paris local time, send an email to `olivier.cappe@ens.fr` and `muni.pydi@lamsade.dauphine.fr` with 2 things: (1) Your top 3 preferences among the provided list of 11 papers (2) the members of the group. Please include all the members of your group in cc of your email.
- By March 6, you will be assigned a paper.
- By March 13, 23:00, send a short progress report ($2-3$ paragraphs) by email to `olivier.cappe@ens.fr`, `muni.pydi@lamsade.dauphine.fr` describing the work done so far, and the planning envisioned for the last two weeks of the project.
- By March 24, 23:00, send your final 6-8 pages report.
- The presentation of the project will be scheduled on March 26, you are expected to attend the whole session devoted to the projects presentation (08:30 to 12:30 on March 26).

Project Papers

1. Accuracy, Interpretability, and Differential Privacy via Explainable Boosting. Harsha Nori, Rich Caruana, Zhiqi Bu, Judy Hanwen Shen, Janardhan Kulkarni. ICML 2021.
2. Bayesian Differential Privacy for Machine Learning. Aleksei Triastcyn, Boi Faltings. ICML 2020.
3. Differentially Private Covariance Estimation. Kareem Amin, Travis Dick, Alex Kulesza, Andres Munoz, Sergei Vassilvitskii. NeurIPS 2019.
4. Differentially Private Quantiles. Jennifer Gillenwater, Matthew Joseph, Alex Kulesza. ICML 2021.

Project Papers

5. Deep Learning with Label Differential Privacy. Badih Ghazi, Noah Golowich, Ravi Kumar, Pasin Manurangsi, Chiyuan Zhang. NeurIPS 2021.
6. Differentially Private Correlation Clustering. Mark Bun, Marek Elias, Janardhan Kulkarni. ICML 2021.
7. Learning Rate Adaptation for Differentially Private Learning. Antti Koskela, Antti Honkela. AISTATS 2020.
8. Choosing Public Datasets for Private Machine Learning via Gradient Subspace Distance. Xin Gu, Gautam Kamath, Zhiwei Steven Wu. TPDP 2023.

Project Papers

9. Easy Differentially Private Linear Regression. Kareem Amin, Matthew Joseph, Monica Ribero, Sergei Vassilvitskii. ICLR 2023.
10. High-Dimensional Private Empirical Risk Minimization by Greedy Coordinate Descent. Paul Mangold, Aurelien Bellet, Joseph Salmon, Marc Tommasi. AISTATS 2023.
11. Differentially Private Heatmaps. Badih Ghazi, Junfeng He, Kai Kohlhoff, Ravi Kumar Pasin Manurangsi, Vidhya Navalpakkam, Nachiappan Valliappan. AAAI 2023.

Useful Links

- Papers with Code - You can search for any paper and find GitHub links to official or unofficial implementations of the code.
- arXiv - Some papers may have an extended version uploaded to arXiv. May have Latex source files too.
- Google Scholar - You can find list of papers that cite a specific paper. Very useful to find follow-up works.
- Semantic Scholar - Alternative to Google Scholar. Can find "highly influenced citations".
- papertalk - Video recordings of conference talks. Can find similar papers also.

Course Evaluation

The homework assignment will constitute 40% of the grade and the project will constitute the remaining 60%.