Class project guidelines

Important note: This assignment is only for students who have signed up for the 3-credit hour course.

The goal of the course project is to provide an opportunity for you to get involved with a current topic of research in learning theory while addressing a computational or societal challenge. You may choose between two types of projects: a survey or original research. For a survey project, you need to write a survey based on four relevant papers. For original research, you need to strive to develop a new model, algorithm, or theorem, or you may focus on experimental results. For further information, see the appropriate sections of this document.

We have the following four assignments regarding the project throughout the semester. For deadlines, see Table 1.

- **Abstract:** For this assignment, write a one-page report outlining your project plans. This report essentially serves as your project proposal. Begin with a brief abstract that captures the essence of your final report, assuming everything proceeds as planned. Within this report, you should clearly define the scope of your project, identify relevant papers in the literature that will serve as your starting points, and describe the initial steps you have already taken. Additionally, explain why you have chosen this particular topic and what motivates studying this topic.
- **Mid-point evaluation:** This a milestone where 40% of your project is done. Think of this assignment as a mini final report. Explain the partial results you may have. What has worked so far and what did not quite work. You need to produce a three-page report for this assignment.
- **Mid-point evaluation:** This is a milestone where you aim to finish $\sim 40\%$ of your project. You need to produce a three-page report for this assignment. Think of this report as a mini final report. Explain the partial results you may have. What has worked so far and what did not quite work.
- **Final report:** Write an eight-page final report for the project. See the relevant sections for more details on what a good project report consists of.
- **Project presentation:** We will have project presentations at the end of the semester.

Policies

Late submission: You will lose 5% of your grade per late day.

Assigment	**Deadline**
Abstract	09/20/2023
Mid-point evaluation	10/18/2023
Final report	11/29/2023
Project presentation	Last two weeks of class: 11/15/2023 and 11/29/2023

Table 1: Assignments and deadlines

Format: Please typeset your reports for these deliveries in Latex and upload them on Canvas by the indicated deadlines.

Group project: You may pair up with another member of the class. However, the expectation for the group projects will be higher accordingly.

Rice Honor Code: You are expected to adhere to the Rice Honor Code. You are encouraged to collaborate and find resources online. However, all the material to be graded is expected to be original unless properly recognized and cited. This policy includes the use of large language models (such as chat-gpt). It is permissible to apply such software for spell/grammar checks to your original text. However, these tools are prohibited for generating content that is not deemed to be yours, including rephrasing others' work and producing summaries.

Surveys

Select a minimum of **four related research papers**, read them carefully, and write a survey. You may choose your own set of papers as long as they are relevant to the topic of the class. A good survey consists of the following:

- **Motivation:** Describe the significant real-world problem that the papers you have chosen aim to address and explain its importance.
- **Literature review:** In addition to the four papers you have selected, compile a comprehensive list of papers related to the topic and explain their differences.
- **Problem definition:** For each paper, provide a clear, formal statement of the problem.
- **Technical overview of the results:** For each paper, provide an overview of their contributions.

- **Comparisons and connections:** This survey should go beyond summarizing papers – it must present the connections between them. For example, explain how one paper builds on another or what novel techniques one paper used that allowed them to overcome barriers others could not.

Below is a list of suggested topics:

Learning threshold functions: On an ordered domain, denoted by X, a threshold function is a function that assigns +1 to all domain elements below a specific threshold value and -1 to the others. Consider the problem of PAC learning threshold functions using labeled samples from this domain. Threshold functions are among the simplest types of functions, and learning them in a non-private setting is straightforward. However, this task becomes surprisingly complex when we add a privacy constraint. In fact, for pure differential privacy, it requires $\Theta(|X|)$ samples. This result implies that learning threshold functions over continuous domains, such as $\mathbb{R}$, is impossible.

In the context of approximate differential privacy (also known as (ϵ, δ)-differential privacy), there has been significant effort to determine the sample complexity of this problem. Seminal work by Bun et al. demonstrates that learning threshold functions requires $\Omega(\log^* |X|)$ samples. After a series of studies, Cohen et al. closed this gap and provided an almost optimal upper bound for the problem. Below is a few papers that studied the problem. For more information, you can explore the references in these papers.

1. Differentially Private Release and Learning of Threshold Functions
   By Mark Bun, Kobbi Nissim, Uri Stemmer, and Salil Vadhan.
   FOCS 2015

2. Private PAC learning implies finite Littlestone dimension
   By Noga Alon, Roi Livni, Maryanthe Malliaris, and Shay Moran.
   STOC 2019

3. Privately Learning Thresholds: Closing the Exponential Gap
   By Haim Kaplan, Katrina Ligett, Yishay Mansour, Moni Naor, and Uri Stemmer.
   COLT 2020

4. Optimal Differentially Private Learning of Thresholds and Quasi-Concave Optimization
   By Edith Cohen, Xin Lyu, Jelani Nelson, Tamás Sarlós, and Uri Stemmer.
   STOC 2023

Privacy and law: Machine learning models consume our digital data to a great extent. The usage of personal data and the chance of accidentally leaking sensitive information have raised worldwide concerns regarding preserving privacy. Several states have instated laws to protect the privacy of individuals, such as the General Data Protection Regulation (GDPR) (a European Union regulation) and the California Consumer Privacy Act (CCPA). Designing algorithms that are compatible with these laws is a crucial task. However, there is a wide gap between the legal/societal expectation and the mathematical/engineering aspect of data privacy. As we have discussed in class, differential privacy (DP) offers a mathematical framework to preserve individuals' privacy. Hence, we can preserve the privacy of individuals while training an ML model, for example. However, this may not be a sufficient level of protection as expected by the law.

One notable example relates to the "right to be forgotten," a protection mandated by certain regulations such as GDPR and CCPA. This legal provision requires that if a user requests the removal of their data, a trained model should 'unlearn' their data points from its training data, as if it were never included in the initial training. One naive approach to abide by these laws is to re-train the model each time a user requests data removal. However, this approach is prohibitively costly. Consequently, substantial research efforts are focused on developing efficient methods that enable data erasure while avoiding the need for model retraining. Here are a few examples:

- Formalizing Data Deletion in the Context of the Right to be Forgotten
  By Sanjam Garg, Shafi Goldwasser, and Prashant Nalini Vasudevan.
  EUROCRYPT 2020

- Remember What You Want to Forget: Algorithms for Machine Unlearning
  By Ayush Sekhari, Jayadev Acharya, Gautam Kamath, and Ananda Theertha Suresh.
  NeurIPS 2021

- Control, Confidentiality, and the Right to be Forgotten
  By Aloni Cohen, Adam Smith, Marika Swanberg, and Prashant Nalini Vasudevan.

- Tight Bounds for Machine Unlearning via Differential Privacy
  By Yiyang Huang, and Clément Canonne.

For another example, see the following paper:

- Towards Formalizing the GDPR's Notion of Singling Out
  By Aloni Cohen and Kobbi Nissim

Statistical-Computational Gap: Studying the optimal number of data points to solve a problem (a.k.a. sample complexity) is the gold standard in statistical learning theory. However, sample complexity is not the only important aspect of the problem; if we cannot find an efficient[1] algorithm that can solve the problem, we are essentially unable to solve it for large instances. Considering these two competing demands raises the following question:

[1] Roughly speaking, we say an algorithm is *efficient* if the time complexity is polynomial in terms of the sample size and other parameters of the problem.

Is there always an efficient algorithm that can solve the problem using the optimal number of samples? Unfortunately, the answer is no. There are several statistical problems where, while theoretically solving the problem is possible, no efficient algorithm exists to do so. Usually, by using more data points, we can efficiently solve the problem. We refer to this discrepancy between the optimal sample complexity and the sample complexity of an efficient algorithm as the *statistical-computational gap*. Formalizing this phenomenon has been the topic of several papers, including:

- Reducibility and Statistical-Computational Gaps from Secret Leakage
  By Matthew Brennan, and Guy Bresler
  See Brennan's thesis here.
- Computational-Statistical Gaps in Reinforcement Learning
  By Daniel Kane, Sihan Liu, Shachar Lovett, and Gaurav Mahajan
- How Hard Is Robust Mean Estimation?
  By Samuel B. Hopkins and Jerry Li
- Robust Sparse Estimation Tasks in High Dimensions
  By Jerry Li

Original research

For the class project, you can work on a novel research problem and either solve it or take steps toward a solution. This could be an extension of your current research or involve proposing experimental verification of an existing result. If you have a problem in mind to propose, that's fantastic. If you need assistance in finding one, I would be happy to share a few problems that I am interested in working on as well. A good final project report for original research consists of the following:

- **Motivation:** Describe what significant real-world problem this research project aims to address and explain its importance.
- **Problem definition:** Provide a clear, formal statement of the problem.
- **Literature review:** Compile a comprehensive list of papers related to your work and explain the advantages and the differences in models or assumptions compared to your work.
- **Technical overview of your results:** Think of this section as what a reviewer would read instead of reading all your proofs. Provide a high-level explanation of your techniques and highlight the significance of your work.

- **Your contributions:** Describe your results in detail here. You may also discuss the techniques you have worked on that did not yield successful results. Try to identify the cases where your solution does or does not work.