COMP 605: Graduate Seminar on Learning Theory

Instructor: Maryam Aliakbarpour

Fall 2024

E-mail: maryama@rice.edu
Office hour: by appointment (email to schedule)
Class: Keith-Wiess 130
Webpage: Click here

Course Description

This course offers an in-depth exploration of the mathematical and computational foundations that underpin the algorithms and models used in machine learning. It is designed to delve into the theoretical aspects of machine learning, covering topics such as statistical learning theory, complexity theory, algorithmic efficiency, and differential privacy. The seminar aims to equip students with a robust understanding of how and why machine learning algorithms work, enabling them to design and implement more effective and efficient models.

Students have the option of registering for a 3-credit hour project, which provides the opportunity to engage with the topic through a project for those seeking a more hands-on experience in the course.

Course Objectives

- Gain insight into state-of-the-art research in learning theory, with a focus on efficient algorithms, differential privacy, and fairness.
- Acquire proficiency in fundamental tools used for mathematical proofs of learning algorithms.
- Practice important soft skills, including reading, understanding, and summarizing scientific papers, evaluating and discussing the strengths and drawbacks of scientific works, and presenting technical content effectively.

Course Format

In this seminar, our aim is to study a collection of papers in learning theory. The class meets weekly for about an hour and 15 minutes, with roughly 13 weeks in the semester.

The instructor will give the first lecture, during which class policies and an overview of the course content will be discussed. The main goal of this lecture is to provide initial information to students so they can choose which paper they would like to present.

The rest of the sessions in the semester will follow the potential timeline below:

- Brief check-in and discussion of what students think of the paper.
- Presentation

Grading Policy

Option 1: This class is one credit hour, and it is graded Satisfactory/Unsatisfactory.

Option 2: This course has the option of being a 3-credit hour course for those who are interested in doing a class project with a letter grade.

To receive a full score, students must complete the following assignments:

- two papers presentation (depending on the number of students in the class maybe two)
- Reading assignments
- Weekly attendance and active participation in class discussions
- Class project (only for the 3-credit hour course)

Paper Presentation: The students should make a 40-minute presentation of a paper in the class. They will sign up for the presentation after the first session. While there is a list of suggested papers, students can present a paper outside of the list as long as it is relevant to the topic of the course, with the approval of the instructor. The students should sign up for one paper presentation (maybe two depending on the size of the class). The presentation should cover the following:

- General motivation and informal statement of the problem
- Brief literature review explaining where this result stands among other work
- Formal problem definition
- Statement of the major results
- Technical part: delve deep into one of the technical results in the paper. The idea here is to learn some technique from the paper that could help us in a theoretical question. We are not necessarily looking for some "difficult" mathematical calculation to present, but rather something reusable or interesting to know. This could be explaining the proof of one of the technical results (or a lemma), or it could be an explanation of some basic concept that was used in the paper.

Reading Assignment: In preparation for the class, the students should read the paper that is presented. Prior to the class, they need to submit a short summary about their paper plus their evaluation. The students will identify the main message of the paper, strengths, drawbacks, and potential follow-up projects.

Class Project (only for the 3-credit hour course): If the student chooses to do a class project, it can be an exploratory research project or a high-quality survey of four relevant papers. Depending on the project, a couple of milestones will be defined for the students during the semester, so they can track their progress and organize accordingly.

Suggested papers

We will primarily study recently published papers that are available online. Here is a list of suggested papers:

1. What Can We Learn Privately?
   Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, Adam Smith
   49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2008)

2. Local Privacy, Data Processing Inequalities, and Statistical Minimax Rates
   John C. Duchi, Michael I. Jordan, Martin J. Wainwright
   26th Annual Conference on Neural Information Processing Systems (NeurIPS 2013)

3. The Composition Theorem for Differential Privacy
   Peter Kairouz, Sewoong Oh, Pramod Viswanath
   Proceedings of the 32nd International Conference on Machine Learning (ICML 2015)

4. A Learning Theory Approach to Noninteractive Database Privacy
   Mark Bun, Kobbi Nissim, Uri Stemmer
   Journal of the ACM (JACM), Vol. 66, No. 2, Article 7 (2019)

5. Smooth Sensitivity and Sampling in Private Data Analysis
   Kobbi Nissim, Sergey Raskhodnikova, Adam Smith
   39th Annual ACM Symposium on Theory of Computing (STOC 2007)

6. Understanding the Sparse Vector Technique for Differential Privacy
   Michael Lyu, David Su, Ninghui Li
   Proceedings of the VLDB Endowment (PVLDB), Vol. 10, No. 6 (2017)

7. Learning Monotone Functions from Random Examples in Polynomial Time
   Ryan O'Donnell, Rocco A. Servedio
   Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC 2008)

8. Robust Estimators in High-Dimensions Without the Computational Intractability
   Ilias Diakonikolas, Gautam Kamath, Daniel Kane, Jerry Li, Ankur Moitra, Alistair Stewart
   48th Annual ACM Symposium on Theory of Computing (STOC 2016)

9. Agnostically Learning Halfspaces
   Adam R. Klivans, Pravesh Kothari, Raghu Meka
   46th Annual ACM Symposium on Theory of Computing (STOC 2014)

10. A New Approach for Testing Properties of Discrete Distributions
    Ilias Diakonikolas, Themis Gouleakis, Ronitt Rubinfeld
    57th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2016)

11. Fundamental Limits of Online and Distributed Algorithms for Statistical Learning and Estimation
    Ohad Shamir
    28th Annual Conference on Neural Information Processing Systems (NIPS 2014)

12. Space lower bounds for linear prediction in the streaming model
    Yuval Dagan, Gil Kur, and Ohad Shamir
    32st Conference on Learning Theory (COLT 2019)

13. Detecting Correlations with Little Memory and Communication
    Yuval Dagan and Ohad Shamir
    31st Conference on Learning Theory (COLT 2018)

14. Efficient Convex Optimization Requires Superlinear Memory
    Annie Marsden, Vatsal Sharan, Aaron Sidford, Gregory Valiant
    35th Conference on Learning Theory (COLT 2022, Best Paper Award)

15. Memory-Sample Tradeoffs for Linear Regression with Small Error
    Vatsal Sharan, Aaron Sidford, and Gregory Valiant
    51st ACM Symposium on Theory of Computing (STOC 2019)

16. Covariance-Aware Private Mean Estimation Without Private Covariance Estimation
    Gavin Brown, Marco Gaboardi, Adam Smith, Jonathan Ullman, and Lydia Zakynthinou
    Conference on Neural Information Processing Systems (NeurIPS 2021, spotlight)

17. When is Memorization of Irrelevant Training Data Necessary for High-Accuracy Learning?
    Gavin Brown, Mark Bun, Vitaly Feldman, Adam Smith, and Kunal Talwar.
    53rd ACM Symposium on Theory of Computing (STOC 2021)

18. Differentially Private Release and Learning of Threshold Functions
    Mark Bun, Kobbi Nissim, Uri Stemmer, and Salil Vadhan
    56th Annual Symposium on Foundations of Computer Science (FOCS 2015).

19. Universality of Computational Lower Bounds for Submatrix Detection
    Matthew Brennan, Guy Bresler, and Wasim Huleihel
    32nd Conference on Learning Theory (COLT 2019)

20. Optimal Average-Case Reductions to Sparse PCA: From Weak Assumptions to Strong Hardness
    Matthew Brennan and Guy Bresler
    32nd Annual Conference on Learning Theory (COLT 2019)

21. Computational-Statistical Gaps in Reinforcement Learning
    Daniel Kane, Sihan Liu, Shachar Lovett, and Gaurav Mahajan

22. Separating Computational and Statistical Differential Privacy (Under Plausible Assumptions)
    Badih Ghazi, Rahul Ilango, Pritish Kamath, Ravi Kumar, and Pasin Manurangsi

23. Inherent Trade-Offs in the Fair Determination of Risk Scores
    Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan

Prerequisites

Students are expected to have a solid understanding of mathematical proofs, basic algorithms, and probability. A course in algorithms or machine learning is recommended as prior preparation.

Course policies

The members of our community at Rice come from many different backgrounds and views. Our goal is to ensure that everyone feels safe, respected, and empowered to be their best selves. We kindly ask our students to treat each other with care and respect.

Rice Honor Code

Students 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.

Disability Resource Center

If you have a documented disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with the Disability Resource Center (Allen Center, Room 111 / adarice@rice.edu / x5841) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs in the first two weeks of class.

Wellbeing and Mental Health

The wellbeing and mental health of students is important; if you are having trouble completing your coursework, please reach out to the Wellbeing and Counseling Center. Rice University provides cost-free mental health services through the Wellbeing and Counseling Center to help you manage personal challenges that threaten your personal or academic well-being. If you believe

you are experiencing unusual amounts of stress, sadness, or anxiety, the Student Wellbeing Office or the Rice Counseling Center may be able to assist you. The Wellbeing and Counseling Center is located in the Gibbs Wellness Center and can be reached at 713-348-3311 (available 24/7).

Title IX Responsible Employee Notification

At Rice University, unlawful discrimination in any form, including sexual misconduct, is prohibited under Rice Policy on Harassment and Sexual Harassment (Policy 830) and the Student Code of Conduct. Please be aware that all employees of Rice University are "mandatory reporters," which means that if you tell me about a situation involving sexual harassment, sexual assault, dating violence, domestic violence, or stalking, we (the course staff) must share that information with the Title IX Coordinator. Although we have to make that notification, you will control how your case will be handled, including whether or not you wish to pursue a formal complaint. Our goal is to make sure you are aware of the range of options available to you and have access to the resources you need. To report sexual harassment, please contact the Title IX Coordinator at titleix@rice.edu. To explore supportive measures and other resources that are available to you, please visit the Office if Interpersonal Misconduct Prevention and Support at safe.rice.edu.