Instructor: Hongyang Zhang
Course number: UWaterloo CS 480/680
Course title: Introduction to Machine Learning
Course website: https://hongyanz.github.io/cs480_680_s23
Class days and time: From May 8 to July 31

- (Session 001) Monday & Wednesday 11:30am-12:50pm
- (Session 002) Monday & Wednesday 1:00pm-2:20pm

Location: MC 2035
Office hours: DC 2641 (or MC 2035), Monday 2:20pm-3:20pm
Contact information: hongyang.zhang@uwaterloo.ca
TAs:

- Chengjie Huang (c.huang@uwaterloo.ca, office hour: Wednesday 11:00am-noon, E7 4418)
- Haochen Sun (haochen.sun@uwaterloo.ca, office hour: Friday 11:00am-noon, DC 3301)
- Yimu Wang (yimu.wang@uwaterloo.ca, office hour: Tuesday 8:00am-9:00am, DC 3301)
- Shufan Zhang (shufan.zhang@uwaterloo.ca, office hour: Thursday 11:00am-noon, DC 3301)

Homework submissions: LEARN
Questions, discussion, and announcements: Piazza
Course description: This course focuses on the introduction of machine leanring. However, we will cover what you are particularly interested in, e.g., technical details of how to train your own ChatGPT. The course will cover four modules of machine learning: (I) Classic ML, (II) Neural Nets, (III) Modern ML Paradigms, and (IV) Trustworthy ML.

Pre-requisite: The course requires basic linear algebra, calculus, probability, algorithm. For example, CM339 / CS341 or SE 240; STAT 206 or 231 or 241.

Requirements:

- Four assignments based on the content of the lectures
- For CS480: Mid-term exam
- For CS680: One course project (each group consists of 1-3 members)
- Final exam

Graded student work for CS480:

- 4 assignments (individual): 40%
- Mid-term exam: 20%
- Final exam: 40%

Graded student work for CS680:

- 4 assignments (individual): 40%
- 1 research project (5% proposal + 25% report, up to 3 members in one group): 30%
- Final exam: 30%

Homeworks (We do not accept hand-written submission; deadline is tentative):

- Assignment 1 (designed by Haochen Sun, posted on May 15) (due by June 4, noon)
- Assignment 2 (designed by Yimu Wang, posted on June 5) (due by June 25, noon)
- Assignment 3 (designed by Chengjie Huang, posted on June 26) (due by July 16, noon)
- Assignment 4 (designed by Shufan Zhang, posted on July 17) (due by Aug 1, noon)

Course Project:

- Proposal (2 pages, NeurIPS template) (due by June 4, noon)
- Final Report (8 pages, NeurIPS template) (due by Aug 1, noon)

Late Policy: We do NOT accept any late submissions, unless you have a legitimate reason with a formal proof (e.g. hospitalization, family urgency, etc.). The proof date should be within 7 days of your homework deadline. Traveling, busy with other stuff, or simply forgetting to submit, are not considered legitimate. Without a proof, you can get at most 75% full score if you are late within 24 hours, and 0 score if you are late beyond 24 hours.

Textbook: There is no required textbook, but the following fine texts are recommended.

- Moritz Hardt and Benjamin Recht. Patterns, Predictions, and Actions. Princeton University Press, 2022.
- Kevin Patrick Murphy. Probabilistic Machine Learning: An Introduction. MIT Press, 2022.
- Steven L. Brunton and J. Nathan Kutz. Data-Driven Science and Engineering Machine Learning, Dynamical Systems, and Control. Cambridge University Press, 2nd edition, 2022.
- Aston Zhang, Zack C. Lipton, Mu Li and Alex J. Smola. Dive into Deep Learning. 2019.
- Ian Goodfellow, Yoshua Bengio and Aaron Courville. Deep Learning. MIT Press, 2016.
- Trevor Hastie, Robert Tibshirani and Jerome Friedman. The Elements of Statistical Learning. Springer, 2017.

Course outline (tentative):

- Introduction
- Perceptron
- Linear Regression
- Logistic Regression
- Hard-Margin SVM
- Soft-Margin SVM
- Reproducing Kernels
- Gradient Descent
- Fully Connected NNs
- Convolutional NNs
- Transformer
- Large Language Models
- GANs
- Self-Supervised Learning
- Evasion Attacks
- Physical and Poisoning Attacks
- Privacy
- Robustness

Academic integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check the Office of Academic Integrity for more information.]

Grievance: A student who believes that a decision affecting some aspect of their university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4. When in doubt, please be certain to contact the department's administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity to avoid committing an academic offence, and to take responsibility for their actions. [Check the Office of Academic Integrity for more information.] A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about "rules" for group work/collaboration should seek guidance from the course instructor,

academic advisor, or the undergraduate associate dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline. For typical penalties, check Guidelines for the Assessment of Penalties.

Appeals: A decision made or penalty imposed under Policy 70, Student Petitions and Grievances (other than a petition) or Policy 71, Student Discipline may be appealed if there is a ground. A student who believes they have a ground for an appeal should refer to Policy 72, Student Appeals.

Note for students with disabilities: AccessAbility Services, located in Needles Hall, Room 1401, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with AccessAbility Services at the beginning of each academic term.
It is the responsibility of the student to notify the instructor if they, in the first week of term or at the time assignment details are provided, wish to submit alternate assignment.

Intellectual Property: Students should be aware that this course contains the intellectual property of their instructor, TA, and/or the University of Waterloo. Intellectual property includes items such as:

- Lecture content, spoken and written (and any audio/video recording thereof);
- Lecture handouts, presentations, and other materials prepared for the course (e.g., PowerPoint slides);
- Questions or solution sets from various types of assessments (e.g., assignments, quizzes, tests, final exams); and
- Work protected by copyright (e.g., any work authored by the instructor or TA or used by the instructor or TA with permission of the copyright owner).

Course materials and the intellectual property contained therein, are used to enhance a student's educational experience. However, sharing this intellectual property without the intellectual property owner's permission is a violation of intellectual property rights. For this reason, it is necessary to ask the instructor, TA and/or the University of Waterloo for permission before uploading and sharing the intellectual property of others online (e.g., to an online repository).
Permission from an instructor, TA or the University is also necessary before sharing the intellectual property of others from completed courses with students taking the same/similar courses in subsequent terms/years. In many cases, instructors might be happy to allow distribution of certain materials. However, doing so without expressed permission is considered a violation of intellectual property rights.
Please alert the instructor if you become aware of intellectual property belonging to others (past or present) circulating, either through the student body or online. The intellectual property rights owner deserves to know (and may have already given their consent).