Instructors:

- Hongyang Zhang (16 lectures)
- Yaoliang Yu (8 lectures)

Course number: UWaterloo CS 480/680, Winter 2024
Course title: Introduction to Machine Learning
Course website: https://watml.github.io/
Class time and locations: From Jan 9 to April 4, 2024:

- (Session 001) Tuesday & Thursday 08:30am-09:50am, MC 2038
- (Session 002) Tuesday & Thursday 10:00am-11:20am, MC 4045
- (Session 003) Tuesday & Thursday 04:00pm-05:20pm, MC 2054

Office hours of instructors: MC 2054, every Tuesday 5:20pm-6:20pm
Contact information:

- Hongyang Zhang, hongyang.zhang@uwaterloo.ca
- Yaoliang Yu, yaoliang.yu@uwaterloo.ca

TAs:

- Haochen Sun (TA head) (h299sun@uwaterloo.ca)
- Ehsan Ganjidoost (eganjidoost@uwaterloo.ca)
- Yanting Miao (y43miao@uwaterloo.ca)
- Alireza Fathollah Pour (a2fathol@uwaterloo.ca)
- Matina Mahdizadeh Sani (m3mahdiz@uwaterloo.ca)
- Shufan Zhang (s693zhan@uwaterloo.ca)

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
- Mid-term exam
- Final exam

Graded student work:

- 4 assignments: 16.66% x 4
- Mid-term exam: 16.66%
- Final exam: 16.7%

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

- Assignment 1 (posted on Jan 11) (due by Feb 8, noon)
- Assignment 2 (posted on Feb 8) (due by March 7, noon)
- Assignment 3 (posted on March 7) (due by March 21, noon)
- Assignment 4 (posted on March 21) (due by April 4, noon)

Completed assignments will be submitted through LEARN. *Submit early and often!*

You must write your solutions independently and individually, and you should always acknowledge any help you get (book, friend, internet, etc.). Using AI to write homeworks is prohibited. We may use tools to detect your submission.

Mark appeals should be requested within two weeks of receiving the mark. The appeal could go either ways, so request only if you truly believe something is wrong.

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, being busy with other stuff, internet disconnection, or simply forgetting to submit, are not considered legitimate. Without a proof, your score will be 0 as long as you are late, even for 1min (LEARN submission portal will be closed on time. We DO NOT accept homework submission by email.). With a proof and instructor's approval, you can get a 7-day homework extension. According to the school policy, undergraduate students are allowed to use short-term absence once per term. Please inform the TA head Haochen Sun (h299sun@uwaterloo.ca) and provide a screenshot if you have submitted an application to Quest for a 2-day extension. Failing to do so (e.g., only informing instructors or other TAs) will make your application invalid, and your delayed howework will still be marked as late.

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

- Tong Zhang. Mathematical Analysis of Machine Learning Algorithms. Cambridge University Press, 2023.
- Moritz Hardt and Benjamin Recht. Patterns, Predictions, and Actions. Princeton University Press, 2022.
- Kevin Patrick Murphy. Probabilistic Machine Learning: An Introduction. MIT Press, 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
- Flow
- Self-Supervised Learning
- Evasion Attacks
- Robustness
- Privacy
- Fairness
- Other Threats

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).