UAB
Universitat Autònoma de Barcelona

Advanced Machine Learning

2026/2027

Code: 106575
Credits: 6

Degree programme	Type	Course
Bachelor in Artificial Intelligence	OP	3

Contact lecturer

Name : Andrey Barsky

Email : andrey.barsky@uab.cat

Group languages

You can consult this information at the end of the document.

Prerequisites

It is strongly recommended to have taken "Fundamentals of Machine Learning" and "Neural Networks and Deep Learning"

Objectives

This subject aims to give a detailed overview of techniques that enhance and optimise neural network models beyond the implementation of task-specific architectures. Building upon the foundation of previous subjects, this course focuses on meta-objectives that transfer, extend, or analyse the operation of existing models.

Students will push their existing understanding of the mechanics of deep learning and address a range of practical challenges in deploying and scaling neural network models in realistic settings. They will learn to train models in resource-constrained settings; probe the behaviour of models to understand their failure cases; learn to subvert models as an adversary, and design models that are secure against subversion.

By the end of this subject, students should have developed skills and expertise to think about secondary objectives in the development of deep models, and be able to reason about the behaviour of neural networks at a high level. They will also have practical experience with these advanced deep learning techniques, equipping them with the knowledge to create systems that are more adaptable, efficient, and robust.

Learning outcomes

- CM07 (Integrate machine learning-based solutions into the design, deployment, and deployment of AI applications.) Integrate machine learning-based solutions into the design, deployment, and deployment of AI applications.
- CM08 (Design machine learning-based solutions that take into account fairness, security, privacy, and transparency criteria while making sustainable use of computing resources.) Design machine learning-based solutions that take into account fairness, security, privacy, and transparency criteria while making sustainable use of computing resources.
- KM23 (Explain the principles and mathematical formulation on which machine learning algorithms are based.) Explain the principles and mathematical formulation on which machine learning algorithms are based.
- KM24 (Identify the advantages and disadvantages of different learning algorithms and paradigms in

their application to learning problems.) Identify the advantages and disadvantages of different learning algorithms and paradigms in their application to learning problems.
- SM25 (Critically and reasoned analysis of the results of the application of a machine learning model according to the requirements of the problem.) Critically and reasoned analysis of the results of the application of a machine learning model according to the requirements of the problem.
- SM26 (Select the appropriate paradigms, algorithms, and architectures for a learning problem, based on the domain and type of problem, the available data, and any other constraints or requirements.) Select the appropriate paradigms, algorithms, and architectures for a learning problem, based on the domain and type of problem, the available data, and any other constraints or requirements.
- SM27 (Efficiently and optimally use the computing resources needed for training and validating learning models.) Efficiently and optimally use the computing resources needed for training and validating learning models.

Contents

Efficient and scalable learning

• Transfer learning and domain adaptation

• Parameter-efficient learning and model compression

• Semi-supervised and self-supervised learning

Advanced learning paradigms

• Ensemble learning and knowledge distillation

• Continual and online learning

• Multi-task and meta learning

Responsible & trustworthy AI

• Explainability & interpretability

• Adversarial robustness and ML security

• Federated learning and ML privacy

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Individual study	20	0.8	CM07, CM08, KM24, SM25, SM26, SM27
Work in projects/exercises	42	1.68	CM07, CM08, KM24, SM25, SM26, SM27
Work in projects/exercises	35	1.4	CM07, CM08, KM24, SM25, SM26, SM27
Laboratory sessions	20	0.8	CM07, CM08, SM26, SM27
Theory classes	20	0.8	KM23, KM24, SM25

Previous modules on machine learning and neural networks have primarily focused on learning theory and practical optimisation to solve specific tasks. In this module, students will learn how to:

• Solve tasks using neural networks under hard design constraints, such as reduced data, reduced computational resources, or complex task requirements

• Solve meta-objectives that transfer or extend the normal operation of models, such as probing the behaviour of models to understand their decision processes, or composing the knowledge of multiple models at once

• Exploit model vulnerabilities to subvert their behaviour, and design models that are secure and robust against such attacks

There will be two types of sessions:

Theory classes: The objective of these sessions is for the teacher to explain the theoretical background of the subject. For each one of the topics studied, the theory and mathematical formulation is explained, as well as the corresponding algorithmic solutions.

Laboratory sessions: Laboratory sessions aim to facilitate interaction, collaborative work and to reinforce the comprehension of the topics seen in the theory classes. During laboratory sessions the students will work through practical cases that require the design of solutions using the methods studied in theory classes. Problem solving will be initiated in the class, but can be continued at home if required.

The above activities will be complemented by a system of tutoring and consultations outside class hours.

Course Project: A course project will be carried out during the second half of the semester, where students will have to solve a specific problem of certain complexity. The students will work in small groups of 2-3 students, where each member of the group must equally contribute to the final solution. These working groups will be maintained until the end of the semester and must be self-managed in terms of distribution of roles, work planning, assignment of tasks, management of available resources, conflicts, etc. To develop the project, the groups will work autonomously, while some of the laboratory sessions will be used (1) for the teacher to present the projects' theme and discuss possible approaches, (2) for monitoring the status of the project and (3) for the teams to present their final results.

All the information of the subject and the related documents that the students need will be available at the virtual campus (cv.uab.cat).

AI Policy: In this subject, the use of Artificial Intelligence (AI) technologies is strongly discouraged within laboratory sessions, as these sessions aim to build theoretical understanding and practical fluency, which is only learned with hands-on effort.

The use of AI technologies is permitted in the context of the course project, for purposes such as coding assistance and text correction, provided that the final result reflects a significant contribution by the student in the analysis and personal reflection. The student must clearly identify which parts have been generated with this technology, specify the tools used and include a critical reflection on how these have influenced the process and the final result of the activity. The lack of transparency in the use of AI will be considered a lack of academic honesty and may lead to a penalty in the grade of the activity, or greater sanctions in serious cases.

Annotation: within the schedule set by the centre or degree programme, 15 minutes of one class will be

reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continuous assessment activities

Title	Weight	Hours	ECTS	Learning outcomes
Delivery of exercises	10%	5	0.2	CM07, CM08, KM24, SM25, SM26, SM27
Delivery of the project	40%	4	0.16	CM07, CM08, KM23, KM24, SM25, SM26, SM27
Written exams	50%	4	0.16	CM08, KM23, KM24, SM25, SM26

To assess the level of student learning, a formula is established that combines theoretical and practical knowledge acquisition, and the ability to solve problems.

Final Grade

The final grade is calculated weighted in the following way and according to the different activities that are carried out:

Final grade = 0.5 * Theory Grade + 0.1 * Problems Portfolio Grade + 0.4 * Project Grade

This formula will be applied as long as the theory and the practical evaluation grades are higher than 5. There is no restriction on the problems portfolio grade. If doing the calculation of the formula yields >= 5 but the theory grade or practical evaluation grade does not reach the minimum required, then a final grade of 4.5 will be given.

Theory Grade

The theory grade aims to assess the individual abilities of the student in terms of the theoretical content of the subject, this is done continuously during the course through two partial exams. The overall theory grade is the average of the grades of the two partial exams.

The mid-term exam (Exam 1) is done in the middle of the semester and serves to eliminate part of the subject if it is passed. The final exam (Exam 2) is done at the end of the semester and serves to eliminate the rest of subject if it is passed.

These exams aim to assess the abilities of each student in an individualized manner, both in terms of solving problems using the techniques explained in class, as well as evaluating the level of conceptualization that the student has made of the techniques seen. In order to obtain a final pass theory grade, it will be required for the both partial exam grades to be higher than 4. If doing the calculation of the formula yields >= 5 but the grades of any of the two partial exams do not reach the minimum required, then the grade for theory that will be used in the final calculation will be 4.5.

Recovery exam. In case the theory grade does not reach the adequate level to pass, the students can take a recovery exam, destined to recover the failed part (1, 2 or both) of the continuous evaluation process.

Problems Portfolio Grade

The aim of the problems (exercises) is for the student to train with the contents of the subject continuously and

become familiar with the application of the theoretical concepts. As evidence of this work, the presentation of a portfolio is requested in which the exercises worked out will be collated.

Project Grade

The course project carries an essential weight in the overall mark of the subject. Developing the project requires that the students work collaboratively and design an integral solution to the defined challenge. In addition, the students must demonstrate their teamwork skills and present the results to the class.

The project is evaluated through its deliverables, an oral presentation that students will make in class, and a self-evaluation process. The participation of students in all three activities (preparing the deliverable, presentation and auto evaluation) is necessary in order to obtain a projects grade. The grade is calculated as follows:

Project Grade = 0.6 * Grade Deliverables + 0.3 * Grade Presentation + 0.1 * Grade Self-evaluation

If performing the above calculation yields >= 5 but the student did not participate in any of the activities (deliverable, presentation, auto evaluation), then a final grade of 4.5 will be given to the course project.

In case the minimum grade is not achieved, the group will be able to recover the project, restricted to a maximum grade of 7/10.

In case of not submitting the project deliverables, not presenting the project, or considering the contents copied or synthetically generated, the course project will be considered failed.

Important notes

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, evaluation activities will be suspended with zero (0) whenever a student commits any academic irregularities that may alter such evaluation (for example, plagiarizing, copying, letting copy, ...). The evaluation activities qualified in this way and by this procedure will not be recoverable. If you need to pass any of these assessment activities to pass the subject, this subject will be failed directly, without opportunity to recover it in the same course.

In case there the student does not deliver any exercise solutions, does not participate in any practical evaluation, and does not take any exam, the corresponding grade will be a \"non-evaluable\". In any other case, the "no shows" count as a 0 for the calculation of the weighted average.

In order to pass the course with honours, the final grade obtained must be equal or higher than 9 points. Because the number of students with this distinction cannot exceed 5% of the total number of students enrolled in the course, it is given to whoever has the highest final marks. In case of a tie, the results of the partial exams will be taken into account.

This module does not provide for the single evaluation system.

More details about the evaluation process will be given at class during the first weeks of the semester. In case of any discrepancy between this guide and the information given at class, the information provided at class takes precedence.

Bibliography

Books:

- Deep Learning, Ian Goodfellow, Yoshua Bengio, and Aaron Courville, MIT Press, 1st Ed. 2016
- Deep learning with Python, François Chollet, Manning Publications, 2nd Ed., 2022
- Pattern Recognition and Machine Learning, Christopher Bishop, Springer, 2011

Online books:

- Michael Nielsen's Neural Networks and Deep Learning
- http://neuralnetworksanddeeplearning.com/
- Zhang, Z.C. Lipton, M. Li, A.J. Smola, "Dive into Deep Learning", 2021
- https://d2l.ai/

Software

For the course practical activities we will use Python (NumPy, MatPlotLib) and PyTorch, taking advantage of computational resources from Google Colab or Kaggle.

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this link. To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(TE) Theory	71	English	first semester	afternoon
(PAUL) Classroom practices	711	English	first semester	afternoon