Universitat Autònoma de Barcelona

**2021/2022**

# Advanced Methods of the Theory of Information and Coding

Code: 104371
ECTS Credits: 6

| Degree | Type | Year | Semester |
|---|---|---|---|
| 2503758 Data Engineering | OT | 4 | 0 |

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

## Contact

Name: Mercè Villanueva Gay

Email: Merce.Villanueva@uab.cat

## Use of Languages

Principal working language: catalan (cat)

Some groups entirely in English: No

Some groups entirely in Catalan: Yes

Some groups entirely in Spanish: No

## Teachers

Joaquim Borges Ayats

Cristina Fernández Córdoba

## Prerequisites

There are no prerequisites. However, students should have either a good mathematical level and be familiar with the concepts of fundamental algebra, or have passed the subject "Teoria de la Informació i de la Codificació".

## Objectives and Contextualisation

The course is focused on coding theory and its applications into the real world. The coding theory is the study of methods for efficient and accurate transfer of information from one place to another. It deals with the problem of detecting and correcting transmission errors caused by noise on the channel. In distributed storage systems, coding theory also offers solutions, to improve hard disk failure tolerance, which are much more efficient than replication-based ones.

## Competences

- Conceive, design and implement efficient and secure data storage systems.
- Generate innovative and competitive proposals in professional activity and research.
- Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
- Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
- Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

## Learning Outcomes

1. Design systems that protect the privacy of personal clinical information in the field of the health sciences.
2. Generate innovative and competitive proposals in professional activity and research.
3. Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
4. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
5. Study the adaptations made to data analysis and consultation algorithms in order for these to maintain the privacy of the entry data, of the models learnt, or of the outputs of the models used in the field of business intelligence.
6. Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

## Content

1. Polynomials and finite fields.

1.1. Rings of integers Z and Z/p.

1.2. Ring of polynomials over Z/p.

1.3. Finite fields GF(p^n)

1. Linear codes over finite fields.

2.1. Introduction to coding theory.

2.2. Generator matrices and equivalent codes

2.3. Orthogonal codes and syndrome decoding

2.4. Hamming codes

1. Cyclic codes over finite fields.

3.1. Introduction to cyclic codes

3.2. Generator polynomial and matrix

3.3. Parity check polynomial and matrix

3.4. Coding and decoding

1. Algebraic codes. BCH and RS codes.

4.1. Introduction and general definitions

4.2. Encoding an algebraic code

4.3. Decoding an algebraic code

4.4. BCH and RS codes

4.5. Correcting errors and/or erasures

1. Applications of error correcting codes

5.1. Error correcting codes in QR, Blu-ray, DVD.

5.2. Error correcting codes in the transmission of information.

5.3. Error correcting codes applied to distributed storage.

5.4. Cryptography based on error correcting codes.

5.5. Error correcting codes applied to watermarking and steganography.

5.6. Error correcting codes used in quantum computation.

## Methodology

The methodology applied to the student work will combine the attended lectures, resolution of examples, and practicum. During the sessions, different concepts will be introduced and the resolution of exercises will be proposed to be solved by the students. The practicum proposals will be guided and will be validated by answering some questions. Campus Virtual will be used for communication between lecturers and students (material, updates, announcements, etc.).

Different activities will be conducted during the course:

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.

## Activities

| Title | Hours | ECTS | Learning Outcomes |
|---|---|---|---|
| Type: Directed | | | |
| Practicum | 12 | 0.48 | 1, 5, 2, 4, 3, 6 |
| Theoretical and practical classes / lectures | 38 | 1.52 | 1, 5, 2, 4, 3, 6 |
| Type: Supervised | | | |
| Practicum supervising | 6 | 0.24 | 1, 5, 2, 4, 3, 6 |
| Tutoring and consultation | 11 | 0.44 | 1, 5, 2, 4, 3, 6 |
| Type: Autonomous | | | |
| Preparing exam | 40 | 1.6 | 1, 5, 2, 4, 3, 6 |
| Preparing exercices and practicum | 35 | 1.4 | 1, 5, 2, 4, 3, 6 |

## Assessment

Continuous-assessment dates will be published on Campus Virtual. Specific programming may change when necessary. Any such modification will always be communicated to students through Campus Virtual, which is the usual communication platform between lecturers and students.

The final evaluation will take into account the portfolio delivered by the students, the attendance and participation in class, and the short oral presentations, as follows:

1. Attendance and active participation. At least 80% of the lectures must be attended. Absences might be compensated with a home-work after agreement with the teacher. Mark: 10%.

2. Exercice resolutions. This is an individual task. As part of continuous assessment, short exercises must be solved. Some will be compulsory, others will be optional. Mark: 25%.
3. Practical activities. Depending on the number of students, it will be an individual task or in groups of two people. These practical activities will be performed by using computers. Mark: 25%.
4. Final exam. This is an individual task. Mark: 40%.

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, assessment activities will receive a zero whenever a student commits academic irregularities that may alter such assessment. Assessment activities graded in this way and by this procedure will not be re-assessable. If passing the assessment activity or activities in question is required to pass the subject, the awarding of a zero for disciplinary measures will also entail a direct fail for the subject, with no opportunity to re-assess this in the same academic year. Irregularities contemplated in this procedure include, among others

- the total or partial copying of an evaluation activity;
- allowing others to copy;
- presenting group work that has not been done entirely by the members of the group;
- presenting any materials prepared by a third party as one's own work, even if these materials are translations or adaptations, including work that is not original or exclusively that of the student;

An overall grade of 5 or higher is required to pass the subject. A "non-assessable" grade cannot be assigned to students who have participated in more than 50% of the exercises and practicum activities or have delivered the oral presentation. No special treatment will be given to students who have completed the course in the previous academic year. In order to pass the course with honours, the final grade must be a 9.0 or higher. Because the number of students with this distinction cannot exceed 5% of the number of students enrolled in the course, this distinction will be awarded to whoever has the highest final grade.

It is important to bear in mind that no assessment activities will be permitted for any student at a different date or time to that established, unless for justified causes duly advised before the activity and with the lecturer's previous consent. In all other cases, if an activity has not been carried out, this cannot be re-assessed.

In the case of exercise resolutions and practical activities, a review may be requested after the date of the activity, allowing students to review the activity with the lecturer. In this context, students may discuss the activity grade awarded by the lecturers responsible for the subject. If students do not take part in this review, no further opportunity will be made available.

To consult the academic regulations approved by the Governing Council of the UAB, please follow this link: http://webs2002.uab.es/afers_academics/info_ac/0041.htm

## Assessment Activities

| Title | Weighting | Hours | ECTS | Learning Outcomes |
|---|---|---|---|---|
| Attendance and active participation | 10 | 0 | 0 | 1, 5, 2, 4, 3, 6 |
| Exam | 40 | 2 | 0.08 | 1, 5, 2, 4, 3, 6 |
| Exercise resolution | 25 | 3 | 0.12 | 1, 5, 2, 4, 3, 6 |
| Practical activities | 25 | 3 | 0.12 | 1, 5, 2, 4, 3, 6 |

## Bibliography


- C. H. Bennett, P. Shor, "Quantum Information Theory", IEEE Trans. Inf. Theory, vol. 44, n.6, pp. 2724-2742, 1998.

- D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), Post-Quantum Cryptography, Springer-Verlag, 2009.

- Thomas M. Cover and Joy A. Thomas (1991). Elements of Information Theory, John Wiley & Sons, Inc.
- K. Gracie and M.-H. Hamon, "Turbo and turbo-like codes: Principles and applications", IEEE Proceedings of in Telecommunications, vol. 95, pp: 1228 - 1254, 2000.
- K. J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, 2007.
- Robert J. McEliece, The Theory of Information and Coding, Addison-Wesley Publishing Co., 1977.
- J. Rifà and Ll. Huguet, Comunicación Digital, Masson Ed. 1991.
- P. Shor, "Algorithms for Quantum Computation: Discrete Logarithm and Factoring", Proceedings 35-th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994.
- Mc. Williams-Sloane: The Theory of Error-Correcting Codes. North-Holland Publishing Company. Amsterdam-N.Y.-Oxford. 1978-1996.


## Software

The practical activities will be perform by using SageMath.
SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more. Access their combined power through a common, Python-based language or directly via interfaces or wrappers. Since version 9.0 released in January 2020, SageMath is using Python 3.