Università degli Studi di L'Aquila - Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica

Course catalogue

Page compiled on 18/08/2019

Programme of Course "Teoria dell'Informazione"

- Code: F0158
- Type of course unit: Elective (Bachelor Degree in Computer Science curriculum General), Elective (Master Degree in Computer Science curriculum GSEEM), Elective (Master Degree in Computer Science curriculum General)
- Level of course unit: Undergraduate Degrees, Postgraduate Degrees
- Semester: 2

Number of ects credits: (Master Degree in Computer Science) 6 (workload 150 hours), (Bachelor Degree in Computer Science) 6 (workload 150 hours)

Teachers: Filippo Mignosi (Filippo.Mignosi@univaq.it)

1	**Course objectives**	The aim of the course is to provide students with the knowledge of some classic aspects of information theory. In particular, topics related to source coding are discussed, including the classical theory of block codes, and data compression but not the topic of channel and noise coding. These last topics are indeed taught in other courses in DISIM. In the second part, elements of modern cryptography are taught. At the end of the lessons, and passing the exam, the student should be able to 1) know the basics of information theory and understand its basic languages ??and notions such as Entropy, Mutual Information, Relative Entropy. 2) To know the first results of Shannon, such as the AEP theorem and their consequences as Shannon's encoding for data compression. To know various types of sources. 3) To know the theory of block codes and the main results of this theory, such as the Kraft McMillan inequality. 4) To know the Huffman coding, the arithmetic coding and to understand the different types of optimality that these encodings represent when they are used on I.I.D. 5) To know the compressors of Lempel and Ziv from 1977 and 1978 and their variants and Elias encodings of integer sequences. With regard to modern cryptography, students must 6) understand discrete probability distributions and be able to apply them in subsequent concepts and results. 7) They must know the initial and basic notions of modern cryptography such as perfect secrecy and one-way function in terms of distributions and 8) must understand the proofs of first theorems. 9) they must also have the ability to calculate the entropy of I.I.D. and of simple Markov chains, knowing how to apply block codes and the compressors studied to simple texts, and in general to be able to use the language of classical information theory in a logical and coherent way even within proofs of theorems. 10) In cryptography students must be able to apply the concepts acquired in classical exercises. Students should also 11) to understand how to apply the concepts of information theory in the real world and to understand that information has always a price. 12) describe the topics of the course with sufficient mathematical rigor, being able to describe the algorithms described in the course completely. Being able to formalize and communicate problems, ideas and solutions. 13) To develop the skills necessary to undertake studies subsequent with a high degree of autonomy. To know how to learn with ease topics, related to the course, of which there is only partial knowledge.
2	**Course content and learning outcomes (dublin descriptors)**	Topics of the module include: • The course is divided into two parts, the first of about four educational credits deals with the source coding in all its possible aspects in classical information theory. The remaining two credits are dedicated to the introduction of modern cryptography. In particular, in the first part we study entropy, mutual information and relative entropy in the case of I.I.D. sources, Jensen's inequality and its consequences. Then we study the AEP theorem and all consequences i.e.bounds both superior and inferior on the probability of the typical set, the Shannon coding for data compression, the definition and properties of the most probable set of minimum cardinality and exercises on the latter. We study the Markov chains and we study how to calculate their entropy and we gives few informations on HMM sources. We study the theory of block codes and the main results of this theory, such as the Kraft McMillan inequality and consequences. The Huffman algorithm is described and its optimality is demonstrated within all the prefix codes. The arithmetic coding is described and the optimality for

		I.I.D. in the sense that convergence to entropy is experienced. The Lempel and Ziv compressors of 1977 and 1978 and their variants and the Elias encodings of sequences of integers are described in order to complete the description of the LZ77 algorithm. As far as modern cryptography is concerned, the initial and basic notions of modern cryptography are given, such as perfect secrecy and one-way function in terms of distributions, and are prooved the first theorems that connect these notions with the classes P and NP. • • On successful completion of this module, the student should : • The aim of the course is to provide students with the knowledge of some classic aspects of information theory. In particular, topics related to source coding are discussed, including the classical theory of block codes, and data compression but not the topic of channel and noise coding. These last topics are indeed taught in other courses in DISIM. In the second part, elements of modern cryptography are taught. At the end of the lessons, and passing the exam, the student should be able to 1. know the basics of information theory and understand its basic languages ??and notions such as Entropy, Mutual Information, Relative Entropy. 2. To know the first results of Shannon, such as the AEP theorem and their consequences as Shannon's encoding for data compression. To know various types of sources. 3) To know the theory of block codes and the main results of this theory, such as the Kraft McMillan inequality. 4) To know the Huffman coding, the arithmetic coding and to understand the different types of optimality that these encodings represent when they are used on I.I.D. 5) To know the compressors of Lempel and Ziv from 1977 and 1978 and their variants and Elias encodings of integer sequences. With regard to modern cryptography, students must 6) understand discrete probability distributions and be able to apply them in subsequent concepts and results. 7) They must know the initial and basic notions of modern cryptography such as perfect secrecy and one-way function in terms of distributions and 8) must understand the proofs of first theorems. 3. they must also have the ability to calculate the entropy of I.I.D. and of simple Markov chains, knowing how to apply block codes and the compressors studied to simple texts, and in general to be able to use the language of classical information theory in a logical and coherent way even within proofs of theorems. 4. In cryptography students must be able to apply the concepts acquired in classical exercises. Students should also 11) to understand how to apply the concepts of information theory in the real world and to understand that information has always a price. 5. describe the topics of the course with sufficient mathematical rigor, being able to describe the algorithms described in the course completely. Being able to formalize and communicate problems, ideas and solutions. 6. To develop the skills necessary to undertake studies subsequent with a high degree of autonomy. To know how to learn with ease topics, related to the course, of which there is only partial knowledge.
3	**Course prerequisites**	Mandatory: To have basic knowledge of probability theory and discrete mathematics.
4	**Teaching methodsand language**	The lessons are usually frontal and few self-assessment “in itinere” tests are carried out which are however completed by frontal explanations. Exercises are done “in class” but their amount is the minimum for developing the ability to apply the acquired knowledge. An attempt is made to make the teaching centered on the students by asking to attending students what do they expect in relation to the course, contents and

		assessment methods. The creation of discussion groups is stimulated both with and without the presence of the teacher regarding the subject of study, and the cross-discussion is stimulated. Students are encouraged to ask questions and develop ability to criticize. Among the teaching methods, motivational techniques such as references to recent news events to arouse interest are also used. The modalities of exams are seen as a didactic method, and indeed, to generate attention, on almost every topics it is explained what are the modalities of exams on that specific topic. **Language**: Italian **Reference textbooks** • Arora, Barak, ***Computational Complexity: A Modern Approach,*** . Cambridge University press . 2009. • Cover e Thomas, ***Elements of Information Theory***. 2006. • Amir Said, ***Introduction to Arithmetic Coding- Theory and Practice***. *https://www.hpl.hp.com/techreports/2004/HPL-2004-76.pdf*
5	**Assessment methods**	A written test is made which is called "interactive". Indeed after the student answered to first questions regarding concepts and basic definitions and tests necessary to pass the exam, the correction is done together with the student himself and, as a general rule, questions are asked according to the answers given, to the precision, to the correctness, to the exposition capacity of the student, and according to the demonstrated logical capacity. This occurs in several similar phases until the commission reaches a judgment deemed valid and reliable. In general, a student must know the basic definitions and basic techniques to pass the exam and then the grade will also grow in proportion to the subjects in which he has been able to answer and also, and we repeat, depending on the answers given. , or rather from the precision, correctness and exposition capacity of the student, from the demonstrated logical capacity. In particular, to assess the ability to apply knowledge and understanding and also the learning skills, students' ability to understand and integrate demonstrations and logical reasoning on 1) topics related to course but which they were not strictly treated as topics of the course or discussion on the most advanced topics in the case of students with an evaluation close to the maximum or 2) topics in which the students expressed uncertainties or inaccuracies to see if they can be more certain or precise. Sometimes a student's self-assessment is also asked for a discussion. Given that the part of the course that deals with modern cryptography is very sophisticated, less weight will be given to inaccuracies and deficiencies on it for the final vote.