Course guides
230358 - BMAC - Basic Mathematics for Algebraic Coding Theory with Applications to Cryptography

Last modified: 29/04/2020

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: MASTER'S DEGREE IN TELECOMMUNICATIONS ENGINEERING (Syllabus 2013). (Optional subject).

Academic year: 2020 **ECTS Credits:** 2.5 **Languages:** English

LECTURER

Coordinating lecturer: Jorge Jimenez

Others: Marcel Fernandez
Jorge Jimenez

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
CE1. Ability to apply information theory methods, adaptive modulation and channel coding, as well as advanced techniques of digital signal processing to communication and audiovisual systems.
CE4. Ability to design and dimension transport, broadcast and distribution networks for multimedia signals
CE8. Ability to understand and to know how to apply the functioning and organization of the Internet, new generation Internet technologies and protocols, component models, middleware and services
CE9. Ability to deal with the convergence, interoperability and design of heterogeneous networks with local, access and core networks, as well as with service integration (telephony, data, television and interactive services).
CE15. Ability to integrate Telecommunication Engineering technologies and systems, as a generalist, and in broader and multidisciplinary contexts, such as bioengineering, photovoltaic conversion, nanotechnology and telemedicine.

Transversal:
CT1a. ENTREPRENEURSHIP AND INNOVATION: Being aware of and understanding how companies are organised and the principles that govern their activity, and being able to understand employment regulations and the relationships between planning, industrial and commercial strategies, quality and profit.

CT2. SUSTAINABILITY AND SOCIAL COMMITMENT: Being aware of and understanding the complexity of the economic and social phenomena typical of a welfare society, and being able to relate social welfare to globalisation and sustainability and to use technique, technology, economics and sustainability in a balanced and compatible manner.

CT3. TEAMWORK: Being able to work in an interdisciplinary team, whether as a member or as a leader, with the aim of contributing to projects pragmatically and responsibly and making commitments in view of the resources that are available.

CT4. EFFECTIVE USE OF INFORMATION RESOURCES: Managing the acquisition, structuring, analysis and display of data and information in the chosen area of specialisation and critically assessing the results obtained.

CT5. FOREIGN LANGUAGE: Achieving a level of spoken and written proficiency in a foreign language, preferably English, that meets the needs of the profession and the labour market.

TEACHING METHODOLOGY

- Lectures
- Application classes
- Exercises
- Oral presentations
- Other activities

LEARNING OBJECTIVES OF THE SUBJECT

Learning objectives of the subject:
The aim of this course is to train the students in the knowledge of the actual mathematics used in coding theory and cryptography. They will learn the most modern applications and will be able to follow new research in engineering security and coding theory.

Learning results of the subject:
- Ability to understand mathematics on finite fields, algebraic curves and basic factorization algorithms as Berlekamp.
- Ability to understand the new algorithms for coding and cryptography
- Ability to analysis current developments in geometric coding theory and its applications to information security
- Ability to analyse, model and apply advanced techniques both security, including cryptographic protocols, as identifying traitors.

STUDY LOAD

Type	Hours	Percentage
Hours large group	20,0	32.00
Self study	42,5	68.00

Total learning time: 62.5 h

CONTENTS

1. Finite fields

Description:
- Properties
- Existence and uniqueness
- Extensions
- Ring of polynomials over finite fields

? Ring of polynomials over finite fields

Full-or-part-time: 12h
Theory classes: 3h
Practical classes: 1h
Self study : 8h

2. Algebraic curves over finite fields

Description:
- Basic properties: smooth and singular curves
- Zeta functions and curves with many rational points, Hasse-Weil Theorem
- Funciton fields
- Riemann Roch
- Examples

Full-or-part-time: 12h
Theory classes: 3h
Practical classes: 1h
Self study : 8h

3. Polynomial Arithmetic

Description:
- Basic arithmetic
- Resultant and discriminants
- Basic Factorization algorithms

Full-or-part-time: 11h
Theory classes: 2h
Practical classes: 1h
Self study : 8h

4. Error Correcting Codes

Description:
- Basics of error correction.
- Polynomial codes. Reed Solomon codes.
- Classical decoding. Berlekamp-Massey Algorithm

Full-or-part-time: 11h
Theory classes: 2h
Practical classes: 1h
Self study : 8h

5. List Decoding

Description:
- List decoding vs Minimum distance decoding
- Guruswami-Sudan algorithm
- Koetter-Vardy algorithm

Full-or-part-time: 12h
Theory classes: 3h
Practical classes: 1h
Self study : 8h

6. Applications of List Decoding

Description:
- Traceability codes
- Tracing algorithms

Full-or-part-time: 4h 30m
Theory classes: 2h 30m
Self study : 2h

GRADING SYSTEM

Exercises: 50%
Oral presentation: 50%

Exercises:
- Description: Exercises to strengthen the theoretical knowledge.
Oral presentation:
- Description: Presentation of a work group.

BIBLIOGRAPHY

Basic:
- McEliece, R. J. Finite fields for computer scientists and engineers. Boston etc.: Kluwer Academic Publishers, 1987. ISBN 0898381916.
- Fernandez, M.; Moreira, J.; Soriano, M. "Identifying Traitors Using the Koetter-Vardy Algorithm". IEEE Transactions on Information Theory [on line]. vol. 57, no. 2, February 2011 [Consultation: 22/11/2016]. Available on: http://ieeexplore.ieee.org/document/5695104/.
- Koetter, R.; Vardy, A. "Algebraic soft-decision decoding of Reed-Solomon codes". IEEE Transactions on Information Theory [on line]. vol. 49, no. 11, November 2003 [Consultation: 22/11/2016]. Available on: http://ieeexplore.ieee.org/document/1246007/.
- Guruswami, V. "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes". IEEE Transactions on Information Theory [on line]. 1999, vol. 45, no. 6, p. 1757-1767 [Consultation: 22/11/2016]. Available on: http://ieeexplore.ieee.org/document/782097/.

RESOURCES

Other resources:
- J.W.P. Hirschfeld, G. Korchmáros & F. Torres, Algebraic Curves over a Finite Field eBook | ISBN: 9781400847419 |
- Judy Walker, ?Codes and Curves?,
Online: http://www.math.unl.edu/ jwalker7/papers/rev.pdf