Engineering Tripos Part IIB, 4F5: Advanced Information Theory and Coding, 2024-25

Module Leader

Prof A Guillen i Fabregas [1]

Lecturer

Prof A Guillen i Fabregas and Dr Jossy Sayir [2]

Timing and Structure

Michaelmas term. 16 lectures. Assessment: 100% exam

Prerequisites

3F7 assumed, 3F1, 3F4 useful but not necessary

Aims

The aims of the course are to:

- Learn about applications of information theory to hypothesis testing as well as refinements of source and channel coding theorems through error exponents.
- Introduce students to the principles of algebraic coding and Reed Solomon coding in particular
- Give students an overview of cryptology with example of techniques that share the same mathematical background as algebraic coding.

Objectives

As specific objectives, by the end of the course students should be able to:

- have gained an appreciation for the connection between information-theoretic concepts and fundamental problems in statistics
- have a good understanding of the derivations of error exponents for data compression and transmission
- have a good understanding of the fundamental connections between hypothesis testing and information theory
- have gained a practical understanding of the algebraic fundamentals that underlie channel coding and cryptology
- understand the properties of linear block codes over finite fields
- be able to implement encoders and decoders for Reed Solomon codes
- have gained an overview of methods and aims in cryptology (including cryptography, crypt- analysis, secrecy, authenticity)
- be familiar with one example each of a block cipher and a stream cipher
- be able to implement public key cryptosystems, in particular the Diffie-Hellman and Rivest- Shamir-Adleman (RSA) systems

Content

This course will introduce students to applications of information theory and coding theory in statistics, information storage, and cryptography.

The first part of the course will discuss applications of information theory to universal data compression, statistics, and inference.

The second part of the course will expand linear coding principles acquired in 3F7 to non-binary codes over finite fields. After establishing the algebraic fundamentals, we will cover Reed-Solomon coding, a technique used in a wide range of communication and storage systems (hard disks, blu ray discs, QR codes, USB mass storage device class, DNA storage, and others.)

The final part of the course will introduce the discipline of cryptology, which includes cryptography, the essential art of ensuring secrecy and authenticity, and cryptanalysis, the dark art of breaking that secrecy. The course will cover a number of methods to provide secrecy, ranging from mathematically provable secrecy to public key methods through which computationally secure communication links can be established over public channels.

Information theory and statistics (7-9L, Prof Albert Guillén i Fàbregas)

- Source coding, optimum fixed-rate coding, error exponents
- Binary hypothesis testing, probability of error, error exponents, Stein's lemma
- M-ary hypothesis testing, probability of error
- Channel coding, connection with hypothesis testing, perfect codes, error exponents

Introduction to practical number theory and algebra (2-3L, Dr Jossy Sayir)

- Elementary number theory
- Groups and fields, extension fields
- 3 equivalent approaches to multiplication in extension fields
- Matrix operations and the Discrete Fourier Transform

Algebraic Coding (3L, Dr Jossy Sayir)

- Linear coding and the Singleton Bound
- Distance profiles and MacWilliams Identities
- Blahut’s theorem
- Reed Solomon (RS) codes
- Encoding and decoding of RS codes

Introduction to Cryptology (2L, Dr Jossy Sayir)

- Overview of cryptology
- Stream ciphers, examples
- Block ciphers, examples
- Public key cryptography, basic techniques

Further notes

Examples papers

Examples papers consist of a recommended list of problems to solve in the lecture notes.

Coursework

none

Booklists

- Information Theory:
  - Elements of Information Theory, T. M. Cover & J. A. Thomas, Wiley-Interscience, 2nd Ed, 2006.
  - Information Theory: Coding Theorems for Discrete Memoryless Systems, I. Csiszàr & J. Körner, Cambridge University Press, 2nd Ed. 2011.
- Coding theory:
  - The Theory of Error-Correcting Codes, F. J. MacWilliams & N. J. A. Sloane, North Holland.
  - Algebraic Codes for Data Transmission, Richard E. Blahut, Cambridge University Press, 2003 (Online 2012)

Please refer to the Booklist for Part IIB Courses for references to this module, this can be found on the associated Moodle course.

Examination Guidelines

Please refer to Form & conduct of the examinations [3].

UK-SPEC

This syllabus contributes to the following areas of the UK-SPEC [4] standard:

Toggle display of UK-SPEC areas.

GT1

Develop transferable skills that will be of value in a wide range of situations. These are exemplified by the Qualifications and Curriculum Authority Higher Level Key Skills and include problem solving, communication, and working with others, as well as the effective use of general IT facilities and information retrieval skills. They also include planning self-learning and improving performance, as the foundation for lifelong learning/CPD.

IA1

Apply appropriate quantitative science and engineering tools to the analysis of problems.

IA2

Demonstrate creative and innovative ability in the synthesis of solutions and in formulating designs.

KU1

Demonstrate knowledge and understanding of essential facts, concepts, theories and principles of their engineering discipline, and its underpinning science and mathematics.

KU2

Have an appreciation of the wider multidisciplinary engineering context and its underlying principles.

D1

Wide knowledge and comprehensive understanding of design processes and methodologies and the ability to apply and adapt them in unfamiliar situations.

E1

Ability to use fundamental knowledge to investigate new and emerging technologies.

E3

Ability to apply mathematical and computer based models for solving problems in engineering, and the ability to assess the limitations of particular cases.

E4

Understanding of and ability to apply a systems approach to engineering problems.

P1

A thorough understanding of current practice and its limitations and some appreciation of likely new developments.

P3

Understanding of contexts in which engineering knowledge can be applied (e.g. operations and management, technology, development, etc).

US1

A comprehensive understanding of the scientific principles of own specialisation and related disciplines.

US4

An awareness of developing technologies related to own specialisation.

Last modified: 23/08/2024 18:37

Links
[1] mailto:ag495@cam.ac.uk
[2] mailto:ag495@cam.ac.uk, js851@cam.ac.uk
[3] https://teaching.eng.cam.ac.uk/content/form-conduct-examinations
[4] https://teaching.eng.cam.ac.uk/content/uk-spec