The University Of Sheffield.

Electronic & Electrical Engineering.

EEE6221 DATA CODING TECHNIQUES FOR COMMUNICATION AND STORAGE

Credits: 15

Course Description including Aims

Processing techniques to enable transmission and storage of data with reliability and security are a key element in nearly all of modern communication systems. This course deals with data coding techniques required for reliable and secure data transmission and storage; it covers various aspects of digital communication tying in elementary communication theory with practical solutions to problems encountered. The aims of this course are :

1. To make students aware of the various techniques available for transmitting binary data, and the situations where each might be appropriate.
2. To look at problems that are associated with signal distortion and the limitations that these impose on a data channel.
3. To examine ways of reliably transmitting information in the presence of non-ideal communication channels.
4. To examine ways of securely transmitting and receiving information over insecure communication channels.
4. To outline various communication architectures in use, referring to practical solutions.
5. To make students aware of some of the communication standards that exist.

Outline Syllabus

Asynchronous Communication : RS232, timing constraints, character framework, standards, UARTs, error checking, modems. **Synchronous Serial Communication :** How it differs from asynchronous communication, biphase codes, Miller codes, ternary codes, advantages, uses, bandwidth requirements, constraint lengths and self clocking ability. **Data Compression:** lossless compression, lossy compression, DCT, JPEG. **Data Integrity:** Error detection, parity check, cyclic redundancy checking, theory and hardware implementation. Error correction, distance, coding gain, BER, soft-decision decoding, Galois fields, algebraic and non-algebraic decoding of block codes. Hamming codes, BCH codes, Reed Solomon codes, software and hardware implementation issues. Covolutional codes, Viterbi decoding, implementation issues. Practical configurations, cross-interleaving, multi-stage coding, serial and parallel concatenation, product codes; introduction to Turbo codes and LDPC codes.
Data Security: security functions and definitions; private key primitives (stream ciphers, AES); public-key primitives (RSA, ECC). Hashes and Random number generators.

Time Allocation

24 lectures plus 12 hours of additional support material.

Recommended Previous Courses

None, although background information equivalent to EEE119, EEE224, and EEE317 “Principles of Communications” would be of value.

Assessment

3 hour examination, answer 4 out of 6 questions.

Recommended Books

Halsall	*Data Communications and Computer Networks*	Addison-Wesley
Stallings	*Data and Computer Networks*	McMillan
Sweeney	*Error Control Coding*	Prentice-Hall
Guy	*Data communications for Engineers*	Macmillan
Bissell	*Digital Signal Transmission*	Cambridge
Houghton	*The Engineer's error coding Handbook*	Chapman & Hall

Objectives

By the end of this module successful students will be able to

1. make sensible choices about the type of communication system that will be required in a given situation, and the type of channel coding that will be best suited to the given environment.
2. display awareness of the sorts of problems that will arise as a result of the design choices made in their solution.
3. demonstrate a working knowledge of the techniques available for combating errors in a given system, and the sorts of errors they will encounter.
4. demonstrate a working knowledge of the techniques available for data compression (both lossy and lossless).
5. show an awareness of some of the communications standard that are provided.
6. describe the basis of data security and be aware of the techniques that exist to encrypt/decrypt data.
7. design a simple error control codec.

Detailed Syllabus

1. Provide a course overview and outline the strengths of the recommended text books.
2. Introduce simple communication concepts using RS232 as an example of asynchronous communication. Character framework, UART.
3. Discuss and calculate timing constraints associated with RS232 and how they affect performance.
4. Modems, amplitude shift keying, phase shift keying, frequency shift keying, biphase, quadrature phase encoding, simple gain × bandwidth / channel capacity theory.
5. Synchronous serial communication. Advantages, penalties, biphase coding schemes. Manchester code, IBM code, Miller coding, Miller^2 coding, DC free codes, constraint lengths, 3B4B codes, bipolar codes including alternate mark inversion (AMI) codes and ternary codes such as 4B3T.
6. Bandwidths and error rates for various codes, and self clocking ability.
7. Data compression, source coding.
8. lossless compression, lossy compression.
9. DCT, DCT-based compression,
10. hybrid-compression, JPEG standard.
11. Data integrity, sources of errors, signal to noise ratio in communication channels, burst errors from impulse noise, burst error length. Vertical and horizontal parity, cyclic redundancy checking.
12. Primitive polynomials, modulo-2 arithmetic. Long hand calculation of CRC from a polynomial,

hardware design of a CRC calculator from a polynomial. Testing the CRC against error patterns.

13. Introduction to error correction using horizontal and vertical parity, uses and limitations. Shannon. Coding gain, error correction as an improvement in channel SNR. Underlying principles of more advanced error correction, Hamming distance.
14. Hamming codes. (Hamming (7,4) codes and generation of a parity check matrix, examples using a parity check matrix). Meggitt decoding.
15. Linear codes. Block codes, Galois fields.
16. BCH codes, encoding and algebraic decoding
17. Reed Solomon codes, encoding and algebraic decoding
18. Frequency domain coding. The Fourier transform over final fields. Advantages of frequency domain coding.
19. Recursive extension and frequency domain decoding of RS codes. Software and hardware implementation issues of BCH and RS codes.
20. Convolutional (trellis) encoders, coding rate, uses. Viterbi decoding
21. Implementation issues of convolutional codes/Viterbi decoding
22. Practical configurations, cross-interleaving, multi-stage coding, serial and parallel concatenation, product codes; introduction to Turbo codes and LDPC codes.
23. Introduction to data security, security functions and definitions;
24. Private key primitives (stream ciphers, AES); public-key primitives (RSA, ECC). Hashes and Random number generators. Hamming codes, BCH codes, Reed Solomon codes, software and hardware implementation issues.

UK-SPEC/IET Learning Outcomes

Outcome Code	Supporting Statement
SM1m / SM1fl	This is achieved by detailed coverage of key data coding techniques resulting in objectives 1, 2, 3, 4, 6 and 7 (see objectives list) that are tested by Examination
SM2m	Detailed understanding of advanced mathematical tools in terms of algebraic manipulations and Galois fields theory underpin the operations and implementation that enable design and efficient implementation of data coding and security primitives treated in this course . These are covered in detail in the course via detailed treatment of examples and their application in the coding methods. These relate to objectives outcomes 3, 4 and 6 and tested by exam.
SM4m	Practical limitations and emerging systems are an important part in the treatment of the coding techniques covered by the course. This is accentuated by the emphasis on the complexity versus performance trade-offs necessary in practice when dealing with implementation of the coding techniques in real life systems. These come under 1, 2 and 5 and are tested by exam.
SM2fl	Practical limitations and emerging systems are an important part in the treatment of the coding techniques covered by the course. This is accentuated by the emphasis on the complexity versus performance trade-offs necessary in practice when dealing with implementation of the coding techniques in real life systems. These are tested by exam.
EA1m / EA1fl	Data transmission/reliability/security/compression principles covered are key to all communications systems and equip the students with the ability to critically

	select or devise the most appropriate technique for a given application (all objectives). This is tested by exam for scenarios not previously covered in the lectures.
EA2m	This is covered in the context of BER, Error detection/correction Performance, Security performance, compression rate and complexity analysis (objectives 1, 2, 3, 4 and 6). This is tested by exam in terms of evaluation of particular schemes.
EA2fl	Galois fields, transmissionreliabilitysecuritycompression principles and their implementation covered in this module are generic and provide solid foundations for innovative solutions. All objectives are geared to lead the student to innovate. Some parts of the exam questions deal with unusual problem scenarios which the students are expected suggest potential solutions.
EA3m	Coverage of Galois Field operation and implementation details; hardware design issues, error detection/correction performance, and BER curves. Tested by examination and relate to all of the 7 listed objectives.
EA5m	Galois fields, transmission/reliability/security/compression principles and their implementation covered in this module are generic and provide solid foundations for innovative solutions. All objectives are geared to lead the student to innovate. Some parts of the exam questions deal with 'unusual' problem scenarios which the students are expected suggest potential solutions.
D2fl	In the context of the topics covered (all objectives). Tested by exam with application to unseen scenarios.
D3p	Covered in concepts of error control coding (objectives 1, 3). Tested by exam.
D3m	Forms the crux of the coding techniques covered to enable reliable/secure communication in noisy environments (objectives 1,2,,3,4,6). Tested by examination.
D7m	This is achieved by the design approach adopted on this course from theory to actual hardware implementation. Relates to objectives 1,2,5, 6 and 7 and tested by exam.
D8m	The design approach adopted in the course is generic in terms of translating a mathematical concept into a practical application with practical limitations. Error control coding and cryptography techniques are an ideal vehicle for teaching design issues starting from advanced mathematical concepts. Exam questions are formulated to accentuate the adopted approach.
D1fl	Forms the crux of the coding techniques covered to enable reliablesecure communication in noisy environments (objectives 1,2,,3,4,6). Tested by examination.
D3fl	The design approach adopted in the course is generic in terms of translating a mathematical concept into a practical application with practical limitations. Error control coding and cryptography techniques are an ideal vehicle for teaching design issues starting from advanced mathematical concepts. Exam questions are formulated to accentuate the adopted approach.
EP9m	This is illustrated as examples describing current and emerging systems and standards.
EP10m	This is covered in terms of examples of existing standards and their application/ implementation in practice.