School of Mathematics

Course 373 — Error Correcting Codes 2005-06
(JS & SS Mathematics)

Lecturer: Dr. M. Purser & Dr. T.G. Murphy

Requirements/prerequisites:

Duration: 21 weeks

Number of lectures per week: 3

Assessment:

End-of-year Examination: 3-hour end of year exam

Description: The course will be in two parts: Dr Purser will lecture on Error Correcting Codes for 2 hours per week, and Dr Murphy will lecture on Finite Fields for 1 hour per week.

The course on Finite Fields can be found on the web at http://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/.

Outline of Dr Purser’s course on Error Correcting Codes

1. Introduction
   - Block codes
   - Hamming distance
   - Errors: Random or Burst
   - Error-detection
   - Probability of Error-detection
   - Error-correction
   - Probability of successful Error-correction
   - Sphere-packing Bound
   - Shannon’s Theorem on Capacity

2. Linear Codes
   - Minimum Weight
   - Generator Matrix
   - Null Matrix
   - Standard Array
   - Syndromes
   - Hamming Codes
   - Perfect Codes
   - Varshamov-Gilbert Bound
• Plotkin Bound
• Non-binary linear Codes
• Erasures

3. Modulation

• Frequency Shift Keying (FSK)
• Phase Shift Keying (PSK)
• Differential PSK (DPSK)
• Symbols and Bits
• Gray Coding
• Noise. Additive White Gaussian Noise (AWGN) and bit errors
• Signal/Noise Ratios (SNRs)
• Shannon for Continuous AWGN Channel
• Shannon Limit
• Other Modulations

4. Cyclic Codes

• Generating Polynomial $g(x)$ of the Ideal
• Systematic Cyclic Codes
• Roots of $g(x)$ and the Null Matrix
• Error-detection with cyclic codes
• Weight distributions
• Shortened Cyclic Codes
• Feed-back shift registers (FBSRs)
• Error-correction with Cyclic Codes, the Syndrome
• Kasami’s Method
• Non-binary Cyclic Codes

5. Information Theory

• Information and Entropy
• Immediate Codes and Compression
• Mutual Information
• Capacity
• The Binary Symmetric Channel (BSC)

6. BCH Codes
• Roots of BCH Codes
• Minimum Polynomials
• Examples
• Error-correction of BCH Codes
• Berlekamp-Massey Algorithm
• Non-binary BCH Codes
• Reed-Solomon Codes
• Weight Distribution and the Probability of Incorrect Error-Correction

7. Convolutional Codes
• Trellis codes
• Viterbi Decoding
• Linear Convolutional Codes
• Catastrophic Codes
• Analysis of Convolutional Codes
• Error-correction
• Soft-decision Decoding
• Sequence, Feedback and Threshold Decoding

8. Trellis Code Modulation (TCM)
• Symbols not bits
• Distance and SNRs
• PSK Example
• Phase Invariance
• Phase/Amplitude Modulation and TCM
• Example

9. Code Division Multiple Access (CDMA)
• Use of Spectrum
• Maximum Length Sequences
• CDMA and Third Generation Mobile Telephony

September 25, 2005