School of Mathematics

MA346D — Finite Fields and Coding theory  
(2011-12) 
(JS & SS Mathematics and TSM )

Lecturer: Dr. Timothy Murphy & Dr. Michael Purser

Requirements/prerequisites:

Duration: Hilary Term (10 weeks)

Number of lectures per week: 3 including tutorials

Assessment:

ECTS credits: 5

End-of-year Examination: 2 hour exam in Trinity Term (May)

Description:

The initial part of the module will be on finite fields by Dr. T. Murphy. 

The last part of the module by Dr. Purser will be about Error-correcting codes and is described in some detail at http://www.maths.tcd.ie/~mpurser/ 

Notes for the finite fields part of the module can be found at http://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/GF.pdf

The topics covered are:

1. The Prime Fields
2. The Prime Subfield of a Finite Field
3. Finite Fields as Vector Spaces
4. Looking for $GF(4)$
5. The Multiplicative Group of a Finite Field
6. Polynomials over a Finite Field
7. The Universal Equation of a Finite Field
8. Uniqueness of the Finite Fields
9. Existence of $GF(p^n)$
10. Automorphisms of a Finite Field
11. Wedderburn’s Theorem
12. Irreducible Polynomials over a Prime Field
13. Irreducible Polynomials over a Prime Field

Appendix A. Galois Theory
Appendix B. The Normal Basis Theorem

In outline the topics on error correcting codes are:

- **Introduction**: Block Codes, Distance, Errors and Probabilities of Detection and Correction
  Sphere-packing Bound; Shannon’s Theorem
  Linear Codes, Weight Generator Matrix, Null Matrix, Standard Array, Syndromes; Non-binary codes

- **Hamming Codes, Perfect Codes**
  Varsharmov-Gilbert and Plotkin Bounds; Modulation, FSK, PSK, DPSK; Symbols and Bits, Gray Coding; Noise, SNRs and relation to error-probabilities; Shannon for AWGN; Erasures

- **Cyclic Codes, Generating Polynomial, Systematic Codes**
  Roots and the Null Matrix; Error-detection, Weight Distribution;
  Feedback Shift Registers: Error-correction with Cyclic Codes, Kasami; Non-binary Cyclic;
  BCH Codes, Roots of Generating Polynomial and distance; Minimum Polynomials; Error-correction with BCH Codes

- **RS Codes**
  Error-correction with RS Codes;
  Performance of RS Codes: Convolutional Codes, Trellises; Decoding and Viterbi; Performance Analysis of Convolutional Codes

- **Trellis Code Modulation**
  Examples with PSK; SNR Gain: Coding for Phase Invariance; Outline of CDMA

January 27, 2012