UNIVERSITY OF DUBLIN

MA3731

TRINITY COLLEGE

Faculty of Science

school of mathematics

JS Mathematics
SS Mathematics

Trinity Term 1998

Course 373

Thursday, June 4 Luce Hall 09.30 — 12.30

Dr. M. Purser and Dr. T.G. Murphy

Answer Section A and B in separate answer books.
Section A - Answer 3 out of the 6 questions
Section B - Answer 2 out of the 4 questions

SECTION A

1. Most block codes are designed to correct random symbol errors. Present *three* methods for using them to correct infrequent bursts of errors of length $\leq r$ bits. Justify your choice of parameters (n, k, d) in each of the three cases, and explain how the error-correction procedures would work.

2. The illustrated circuit generates a $\frac{1}{3}$-rate convolutional code: for each new bit input three bits are output. What is the distance of the code?

   If 000000111000101100101001011110 is received, what was sent? (The most left-hand bit is the first bit, corresponding to output 1 on the diagram.)

   1

   2

   3

   $\frac{1}{2}$-rate codes can be generated if one of the three outputs is omitted. For each of the three $\frac{1}{2}$-rate codes so obtained find the distance, and make any relevant observations on the "goodness" or otherwise of the code.

3. State Shannon's theorem relating code-rate to capacity for error-free communication, and prove it. What assumptions underline your proof?
   Why is it important to have large values of n, the length of codewords, for the validity of the theorem and for the performance of codes near the Shannon limit?

4. Define the concept of a syndrome in block codes. Show that correctable errors have distinct syndromes.

   How are syndromes evaluated in terms of the roots of the generator polynomial of cyclic codes, $g(x)$? Present the null matrix $\mathbf{H}$ in terms of the roots of $g(x)$, and reconcile the number of rows $(n-k)$ of $\mathbf{H}$, with the degrees of the irreducible factors of $g(x)$.

   Suppose $S(\alpha)$ denotes the (partial) syndrome calculated from root α of $g(x)$, show that $S(\alpha^2) = (S(\alpha))^2$ for binary codes. Is this true for non-binary codes?

   Suppose $\mathbf{H}$ is in systematic form. Does this affect the actual values of the syndromes? Discuss.

   Illustrate your answer by considering

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1).$$

5. Derive a formula for the length, n, of a binary cyclic code with

$$g(x) = \Pi p_i(x) \qquad 1 \leq i \leq r$$

   where $p_i(x)$ is an irreducible polynomial of degree m_i over $GF(2)$.
   If α is a primitive root of $(x^n - 1)$ with $n = 2^{11} - 1$ what are the roots of the minimum polynomial $m(x)$ of $\beta = \alpha^{89}$? What is the degree of $m(x)$? What is the order of β. Let $m(x)$ be the generating polynomial of an (n, k) cyclic code; what do you suppose the distance of that code to be? What values have n and k? Sketch the standard array for the code. Does this cause you to revise your estimate of this distance? Discuss.

6. The polynomial

$$g(x) = x^5 + \alpha x^4 + \alpha x^3 + \alpha^3 x^2 + x + \alpha^3$$

   defines an RS code over $GF(2^3)$. ($GF(2^3)$ is represented by powers of α, a primitive root of $(x^3 + x + 1)$; with, for example, (110) meaning $(\alpha^2 + \alpha + 0) = \alpha^4$)
   What are the roots of $g(x)$?
   The vector (010011001011000000000) is received.
   Correct it.
   What would you expect to happen if you were asked to correct (010011001000000000000)?
   Does it? Explain what is going on.

SECTION B

7. Show that the multiplicative group $F^\times = F - \{0\}$ of a finite field F is cyclic.

   Find all the generators of $\mathbf{GF}(17)^\times$.

   Determine the number of generators of $\mathbf{GF}(2^{16})^\times$.

8. Define the *characteristic* of a field, and show that the characteristic of a finite field F is always a prime number.

   Show that if F is a field of characteristic p then the map

   $$\Phi : x \mapsto x^p$$

   is an automorphism of F; and show that every automorphism of F is of the form $x \mapsto \Phi^i(x)$ for some i.

9. Show that the number of elements in a finite field is necessarily a prime-power p^n; and prove that there exists just one finite field $\mathbf{GF}(p^n)$ of each such order, up to isomorphism.

10. Show that if $f(x)$ is a prime (irreducible polynomial) of degree d over $\mathbf{GF}(p)$, then

    $$f(x) \mid x^{p^d} - x.$$

    Hence or otherwise show that if there are $N(d,p)$ prime polynomials of degree d over $\mathbf{GF}(p)$ then

    $$\sum_{d|n} dN(d,p) = p^n.$$

    Determine the number of prime polynomials of degree 7 over $\mathbf{GF}(2)$, and find one of them.