Finite Fields (Coding Theory I)

Sample Exam

April 1990

Answer as many questions as you can; all carry the same number of marks.
The term 'field' means commutative field*.*

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

   Find all generators of $\mathbf{GF(13)}^\times$.

   Listing the elements of $\mathbf{GF(16)}$ in any way you wish, define the addition and multiplication in this field.

2. 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.

3. What is meant by saying that a polynomial over a field is *prime* (or irreducible)?

   State and prove the Prime Factorisation Theorem for polynomials over a field.

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

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

Determine the number of prime polynomials of degree 6 over $\mathbf{GF(2)}$, and find one of them.

4. Let F be a finite field. Define the *prime subfield* of F, and its *characteristic*; and show that the characteristic is always a prime.

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

   $$\pi : x \mapsto x^p$$

   is an automorphism of F; and show that the automorphism group of F is a finite cyclic group generated by π.

   Prove that F has possesses at least one *normal basis* over its prime subfield, consisting of an element of F and all its conjugates (transforms under automorphisms).

5. Show that it is always possible to construct a binary (n, k) linear code with minimum distance d provided that

   $$k \le n\left(1 - H\left(\frac{d-2}{n-1}\right)\right) \qquad \text{for large } n$$

   where $H(\lambda)$ is the entropy function

   $$H(\lambda) = \lambda \log_2(1/\lambda) + (1-\lambda)\log_2\left(1/(1-\lambda)\right).$$

6. Why has a Hamming code a length n which is odd?

   Show how a Hamming code can be extended to have length $(n+1)$ and even parity, using the $(7, 4)$ code as an example. How does this extension affect the minimum distance?

   What are the syndromes corresponding to simple bit errors of the $(7, 4)$ and $(8, 4)$ codes?

7. Define a BCH code in terms of the roots of the generating polynomial, and prove its distance properties.

   Give an example of a BCH code with minimal distance $d = 7$.

8. A $(7,3)$ Reed-Solomon code on $\mathbf{GF(2^3)}$ has as roots of its generating polynomial $1, \alpha, \alpha^2, \alpha^3$ where α is a primitive member of $\mathbf{GF(2^3)}$ (e.g. a root of $(x^3{+}x{+}1)$ over $\mathbf{GF(2)}$). The vector $(1, \alpha^2, \alpha^2, \alpha^4, \alpha^5, \alpha^5, \alpha^3)$ was received from a communication channel. By calculating the syndromes S_1, S_2, S_3, S_4 and solving the equations

$$\begin{aligned} S_3 + \sigma_1 S_2 + \sigma_2 S_1 &= 0 \\ S_4 + \sigma_1 S_3 + \sigma_2 S_2 &= 0 \end{aligned}$$

where $\sigma(x) \equiv x^2 + \sigma_1 x + \sigma_2$ has as roots the error locators X_1, X_2; find the locations and the values of the errors, and hence reconstruct the transmitted vector.