UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday 9 June 2003 1.30 to 3.30

PAPER 36

ALGEBRAIC CODING

Attempt **THREE** *questions.*

There are **four** *questions in total.*

The questions carry equal weight.

Candidates may bring into the examination any lecture notes made during the course, printed lecture notes, example sheets and model solutions, and books or their photocopies.

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 Define the dual $\mathcal{X}^{\perp}$ of a linear $[n, k]$ code of length n and dimension k with alphabet $\mathbb{F}$. Prove or disprove that if $\mathcal{X}$ is a binary $[n, \frac{n-1}{2}]$ code with n odd then $\mathcal{X}^{\perp}$ is generated by a basis of $\mathcal{X}$ plus the word $1 \dots 1$. Prove or disprove that if a binary code $\mathcal{X}$ is self-dual: $\mathcal{X} = \mathcal{X}^{\perp}$ then n is even and the word $1 \dots 1$ belongs to $\mathcal{X}$.

Prove that a binary self-dual linear $[n, \frac{n}{2}]$ code $\mathcal{X}$ exists for each even n. Conversely, prove that if a binary linear $[n, k]$ code $\mathcal{X}$ is self-dual then $k = \frac{n}{2}$.

Give an example of a non-binary linear self-dual code. Justify your answer.

2 Define a finite field $\mathbb{F}_q$ with q elements and prove that q must have the form $q = p^s$ where p is prime integer and $s \geqslant 1$ positive integer. Check that p is the characteristic of $\mathbb{F}_q$.

Prove that for any p and s as above there exists a finite field $\mathbb{F}_p^s$ with p^s elements, and this field is unique up to isomorphism.

Prove that the set $\mathbb{F}_{p^s}^*$ of the non-0 elements of $\mathbb{F}_{p^s}$ is a cyclic group $\mathbb{Z}_{p^s-1}$.

Write the field table for $\mathbb{F}_9$, identifying the powers β^i of a primitive element $\beta \in \mathbb{F}_9$ as vectors over $\mathbb{F}_3$. Indicate all vectors α in this table such that $\alpha^4 = e$.

3 What is an $(n, \mathbb{F}_q)$-root of unity? Show that the set $\mathbb{E}^{(n,q)}$ of the $(n, \mathbb{F}_q)$-roots of unity form a cyclic group. Check that the order of $\mathbb{E}^{(n,q)}$ equals n if n and q are co-prime. Find the minimal s such that $\mathbb{E}^{(n,q)} \subset \mathbb{F}_{q^s}$.

Define a primitive $(n, \mathbb{F}_q)$-root of unity. Determine the number of primitive $(n, \mathbb{F}_q)$-roots of unity when n and q are co-prime. If ω is a primitive $(n, \mathbb{F}_q)$-root of unity, find the minimal ℓ such that $\omega \in \mathbb{F}_{q^\ell}$.

Find all $(4, \mathbb{F}_9)$ roots of unity as vectors over $\mathbb{F}_3$.

4 Give the definition of a cyclic code of length n with alphabet $\mathbb{F}_q$. What are the defining zeros of a cyclic code and why are they always $(n, \mathbb{F}_q)$ roots of unity? Prove that the ternary Hamming $[\frac{3^s-1}{2}, \frac{3^s-1}{2} - s, 3]$ code is equivalent to a cyclic code and identify the defining zeros of this cyclic code.

A sender uses the ternary $[13, 10, 3]$ Hamming code, with field alphabet $\mathbb{F}_3 = \{0, 1, 2\}$ and the parity-check matrix

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 2 & 0 \\ 1 & 2 & 1 \\ 1 & 2 & 2 \end{pmatrix}.$$

The receiver receives the word

$$2\ 1\ 2\ 0\ 1\ 1\ 0\ 0\ 2\ 1\ 1\ 2\ 0.$$

How should he decode it?