UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 14 June, 2005 1.30 to 3.30

PAPER 87

ALGEBRAIC CODING

*Attempt **ALL** questions.*

*There are **THREE** questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

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

1 The binary Golay $[24, 12]$ code $\mathcal{X}_{24}^{(\mathrm{G})}$ is determined by its generating matrix $G = (I_{12}|A)$ where I_{12} is a 12×12 identity matrix, and

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Check that $\mathcal{X}_{24}^{(\mathrm{G})}$ is a self-dual code generated by $(A|I_{12})$. Prove that the minimum distance $d(\mathcal{X}_{24}^{(\mathrm{G})}) = 8$. Define the binary Golay $[23, 12]$ code $\mathcal{X}_{23}^{(\mathrm{G})}$ and prove that it is perfect.

Suppose you received a binary word $y \in \mathcal{H}_{24}$, and the syndrome yH has weight $w(yH) \geqslant 3$. Here $H = \begin{pmatrix} I_{12} \\ A \end{pmatrix}$ is the parity-check matrix of $\mathcal{X}_{24}^{(\mathrm{G})}$. How would you decode y in code $\mathcal{X}_{24}^{(\mathrm{G})}$?

2 In this example, $\mathcal{H}_n = \mathcal{H}_{n,q}$ stands for the Hamming space of length over a finite field $\mathbb{F}_q$ where q is a power of a prime number. Define a cyclic code $\mathcal{X} \subseteq \mathcal{H}_n$ and show how to associate with $\mathcal{X}$ and ideal in the quotient ring $\mathbb{F}_q[X]/\langle X^h - e \rangle$. Define the minimum degree generator $g(X)$ of the cyclic code and show that $(X^n - e)|g(X)$. Define the zeros $\alpha_1, \ldots \alpha_u$ of the cyclic code and show how to write its parity-check matrix in terms of $\alpha_1, \ldots, \alpha_u$.

Verify that for $q = 2$, the Hamming $[2^s - 1, 2^s - s - 1, 3]$ code is equivalent to a cyclic code and identify the corresponding minimum degree generator $m_\omega(X)$ and zeros $\omega, \omega^2, \ldots, \omega^{2^S - 1}$.

3 What is a $q-$ary Reed-Solomon (RS) code? Check than an RS code is cyclic and identify its generator.

Define a maximum distance separable (MDS) code and prove that an RS code is MDS. Check that the dual of an RS code is an RS code. Describe, without proofs, the encoding and decoding procedures for RS codes in terms of a primitive $(q - 1, \mathbb{F}_q)$ root of unity.

END OF PAPER