UNIVERSITY OF ABERDEEN **SESSION 2005-06**

DEGREE EXAMINATION

MX4533 Applications of Algebra

Friday 26 May 2006 (9 am—11 am)

Only calculators approved by the Department of Mathematical Sciences may be used in this examination. Calculator memories must be clear at the start of the examination.

Marks may be deducted for answers that do not show clearly how the solution is reached.

Answer THREE questions. All questions carry equal weight.

1. **(a)** Fix $m \geq 2$. Define the binary Hamming code $H(m)$ of length $2^m - 1$. Construct a codeword of weight 3 in $H(m)$. Prove that the minimum distance of $H(m)$ is exactly 3.

(b) We represent the field $\mathbb{F}_8$ as the quotient $\mathbb{F}_2[T]/(m)$ where $m(T) = T^3 + T^2 + 1$. Show that the element $\beta = (T \mod m(T))$ is a primitive element of $\mathbb{F}_8$.

Consider the binary Hamming code $H(3)$ of length 7 defined by β in $\mathcal{R}_3 = \mathbb{F}_2[X]/(X^7 - 1)$. Decode (i.e. find the nearest neighbour of) $f(X) = X^6 + X^5 + 1$. Justify your answer.

2. **(a)** What is the Frobenius automorphism of $\mathbb{F}_{p^n}$? When are two elements α and α' of $\mathbb{F}_{p^n}$ called Galois conjugate?

(b) Let $f \in \mathbb{F}_p[X]$ be the minimal polynomial of an element $\beta \in \mathbb{F}_{p^n}$ and let m denote $\deg f(X)$. Show that β has exactly m Galois conjugates $\alpha_1, \ldots, \alpha_m$ and that $f(X) = \prod_{i=1}^{m}(X - \alpha_i)$.

(c) Let β denote a primitive 9-th root of unity over $\mathbb{F}_2$. Use powers of β to express the 9-th roots of unity and determine their Galois conjugacy classes. Show that $X^9 + 1$ has 3 irreducible factors of degrees $1, 2$ and 6. Show that the divisor $g(X) = X^7 + X^6 + X^4 + X^3 + X + 1$ generates a code C of dimension 2 in $\mathcal{R}_9 = \mathbb{F}_2[X]/(X^9 - 1)$. What is the weight of $g(X)$? Show that C is a BCH code of designed distance 6 and deduce that the minimum distance of C is 6.

3. **(a)** Define the q-ary Reed-Solomon code $\mathrm{RS}(q, k)$ of dimension k.
Prove that it is a BCH code of designed distance $q - k$ and show that this is in fact the minimum distance d of this code.

(b) Fix a positive integer n not divisible by the prime p where $q = p^m$. Let $\mathcal{R}_n$ denote the ring $\mathbb{F}_q[X]/(X^n - 1)$. Prove that X is an invertible element in $\mathcal{R}_n$.
Fix a primitive n-th root of unity β over $\mathbb{F}_q$ and recall that the Mattson-Solomon polynomial of $a(X) \in \mathcal{R}_n$ is defined by $a^{\#}(X) = \sum_{j=1}^{n} a(\beta^j) X^{n-j}$. Show that $a(X) = n^{-1} \cdot a^{\#\#}(X^{-1})$.
You may use without proof the fact that for any integer k

$$\sum_{j=0}^{n-1} \beta^{kj} = \begin{cases} n & \text{if } n|k \\ 0 & \text{otherwise} \end{cases}$$

(c) Show that $T : \mathcal{R}_{q-1} \to \mathcal{R}_{q-1}$ defined by $T : a(X) \mapsto a^{\#}(X)$ carries $\mathrm{RS}(q, k)$, where $k \leq q - 1$, onto the subspace of polynomials in $\mathcal{R}_{q-1}$ of degree $< k$.

4. **(a)** Fix a vector space V over $\mathbb{F}_q$.
What is the support of a function $f : V \to \mathbb{F}_q$?
What is the Hamming distance between two functions $f, g : V \to \mathbb{F}_q$?
Define the Reed-Muller code $\mathrm{RM}(q, m)$ over $V = \mathbb{F}_q^m$.

(b) Show that the Reed-Muller code $\mathrm{RM}(q, m)$ has

(i) One codeword of weight 0,

(ii) $q - 1$ codewords of weight q^m, and

(iii) $q^m - q$ codewords of weight $q^m - q^{m-1}$.

Show that the minimum distance of $\mathrm{RM}(q, m)$ is $q^m - q^{m-1}$.

(c) Fix $m = 3$ and $q = 2$ and arrange the vectors of $V = \mathbb{F}_2^3$ using the binary number trick, namely, $V = \{\mathrm{v}_0, \ldots, \mathrm{v}_7\}$ where $\mathrm{v}_i = (v_0, v_1, v_2)$ represents i as a binary number. So

$$\mathrm{v}_0 = \begin{pmatrix}0\\0\\0\end{pmatrix}, \qquad \mathrm{v}_1 = \begin{pmatrix}0\\0\\1\end{pmatrix}, \qquad \mathrm{v}_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}, \qquad \cdots, \qquad \mathrm{v}_7 = \begin{pmatrix}1\\1\\1\end{pmatrix}.$$

How many errors can $C = \mathrm{RM}(2, 3)$ correct? Consider a function $f : V \to \mathbb{F}_2$ given by

v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7
1	1	0	0	0	1	0	0

Decode f, i.e find its nearest neighbour in C. You may use the following calculations where e_1, e_2, e_3 denote the standard basis of V

$$\begin{aligned}
f(\mathrm{v}_0 + e_1) - f(\mathrm{v}_0) &= f(\mathrm{v}_1) - f(\mathrm{v}_0) = 0\\
f(\mathrm{v}_2 + e_1) - f(\mathrm{v}_2) &= f(\mathrm{v}_3) - f(\mathrm{v}_2) = 0\\
f(\mathrm{v}_4 + e_1) - f(\mathrm{v}_4) &= f(\mathrm{v}_5) - f(\mathrm{v}_4) = 1\\
f(\mathrm{v}_6 + e_1) - f(\mathrm{v}_6) &= f(\mathrm{v}_7) - f(\mathrm{v}_6) = 0
\end{aligned}$$

$$\begin{aligned}
f(\mathrm{v}_0 + e_2) - f(\mathrm{v}_0) &= f(\mathrm{v}_2) - f(\mathrm{v}_0) = 1\\
f(\mathrm{v}_1 + e_2) - f(\mathrm{v}_1) &= f(\mathrm{v}_3) - f(\mathrm{v}_1) = 1\\
f(\mathrm{v}_4 + e_2) - f(\mathrm{v}_4) &= f(\mathrm{v}_6) - f(\mathrm{v}_4) = 0\\
f(\mathrm{v}_5 + e_2) - f(\mathrm{v}_5) &= f(\mathrm{v}_7) - f(\mathrm{v}_5) = 1
\end{aligned}$$

$$\begin{aligned}
f(\mathrm{v}_0 + e_3) - f(\mathrm{v}_0) &= f(\mathrm{v}_4) - f(\mathrm{v}_0) = 1\\
f(\mathrm{v}_1 + e_3) - f(\mathrm{v}_1) &= f(\mathrm{v}_5) - f(\mathrm{v}_1) = 0\\
f(\mathrm{v}_2 + e_3) - f(\mathrm{v}_2) &= f(\mathrm{v}_6) - f(\mathrm{v}_2) = 0\\
f(\mathrm{v}_3 + e_3) - f(\mathrm{v}_3) &= f(\mathrm{v}_7) - f(\mathrm{v}_3) = 0
\end{aligned}$$

Justify your answer.