UNIVERSITY OF ABERDEEN **SESSION 2004-05**

DEGREE EXAMINATION
MX4533 Applications of Algebra
Friday 27 May 2005 (12 noon—2 pm)

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)** When are two vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbb{F}_q^n$ said to be orthogonal ? Define the dual code $C^\perp$ of a q-ary code C of length n. What is the relation between the dimensions of C and $C^\perp$?
(b) Let $h(X)$ be a polynomial over $\mathbb{F}_q$ of degree $< q-1$. Show that

$$\sum_{\alpha \in \mathbb{F}_q} h(\alpha) = 0.$$

(c) The q-ary Reed-Solomon code $\mathrm{RS}_q(k)$ of dimension k is a subspace of $\mathrm{Func}(\mathbb{F}_q, \mathbb{F}_q) = \{f : \mathbb{F}_q \to \mathbb{F}_q\}$ consisting of all the polynomial functions of degree $< k$. Define the inner product $\langle f, g \rangle$ of two elements f, g in $\mathrm{Func}(\mathbb{F}_q, \mathbb{F}_q)$. Show that $\mathrm{RS}_q(k)^\perp = \mathrm{RS}_q(q-k)$.

2. **(a)** Define the weight enumerator polynomial $W_C(X,Y)$ of a q-ary code C of length n.

(b) Let $\mathbb{F}_q$ be a finite field of characteristic p. What is a character of the additive group $(\mathbb{F}_q, +)$?

Prove that if χ is a character then

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha) = \begin{cases} q & \text{if } \chi \text{ is trivial} \\ 0 & \text{if } \chi \text{ is not trivial.} \end{cases}$$

(c) Consider the q-ary code C of length n whose check matrix is $H = \underbrace{(1, 1, \ldots, 1)}_{n \text{ times}}$. Write down a generator matrix for $C^\perp$ and show that

$$C^\perp = \{(t, t, \ldots, t) : t \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n.$$

What is $W_{C^\perp}(X,Y)$? Use the MacWilliams identity

$$W_{D^\perp}(X,Y) = \frac{1}{q^{\dim D}} W_D(X + (q-1)Y, X - Y)$$

to find $W_C(X,Y)$. How many codewords of weight j are there in C $(j = 0, \ldots, n)$?

3. **(a)** When is a q-ary code C of length n called cyclic ?

(b) Recall that we identify the vector space $\mathbb{F}_q^n$ with the quotient ring $\mathbb{F}_q[X]/(X^n - 1)$ via

$$(a_0, a_1, \ldots, a_{n-1}) \quad \leftrightarrow \quad a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}.$$

Prove that a code C in $\mathbb{F}_q[X]/(X^n - 1)$ is cyclic if and only if C is an ideal in $\mathbb{F}_q[X]/(X^n - 1)$.

(c) Determine the generator polynomials and dimensions of all the binary cyclic codes of length 7. You may use, without proof, the factorization into irreducible polynomials

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

4. **(a)** Define what a q-ary BCH code of length n and designed distance δ is.

(b) Prove that the minimum distance of a q-ary BCH code C of designed distance $\delta \leqslant h$ and length n, where $\gcd(n, q) = 1$, is at least δ.

(c) Fix $n = 7$ and $q = 2$ and let β be a primitive 7th root of unity in some field extension of $\mathbb{F}_2$. Use the following factorization into irreducible polynomials over $\mathbb{F}_2$

$$\begin{aligned} &X^7 - 1 = m_1(X) m_3(X) m_7(X) \qquad \text{where} \\ &m_1(X) = (X - \beta)(X - \beta^2)(X - \beta^4) \\ &m_3(X) = (X - \beta^3)(X - \beta^6)(X - \beta^5) \\ &m_7(X) = X - \beta^7 = X - 1 \end{aligned}$$

to find a generator polynomial of a binary BCH code of length 7 and designed distance $\delta = 4$ whose dimension is $k = 3$.