UNIVERSITY OF ABERDEEN **SESSION 2003–04**

DEGREE EXAMINATION
MX4533 Applications of Algebra
Wednesday 26 May 2004 (3pm to 5pm)

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.

The following notation will be used

⋆ q denotes the number of elements in a finite field $\mathbb{F}_q$. Thus, $q = p^m$ for some prime p.

⋆ $\Gamma(S;\mathbb{F}_q)$ denotes the vector space of all functions $f : S \to \mathbb{F}_q$ where S is a given finite set.

⋆ w denotes the weight function

⋆ the dot product of vectors in $\mathbb{F}_q^n$ is denoted by $\underline{u} \bullet \underline{v}$.

1. **(a)** Define a *generator matrix* of a code. Explain what is meant by a *self-dual code*.

(b) Consider a binary **self dual** code $C \subseteq \mathbb{F}_2^n$. Show that $\underline{v} \bullet \underline{v} = 0$ for every $\underline{v} \in C$ and deduce that $w(\underline{v})$ is even.

(c) Given a self dual code C, use **(b)** to show that the weight enumerator polynomial $W_C(X,Y)$ of C satisfies

(i) $W_C(X,Y) = W_C(X,-Y)$ (ii) $W_C(X,Y) = W_C(\frac{X+Y}{\sqrt{2}}, \frac{X-Y}{\sqrt{2}})$

and deduce from (i) and (ii), or show otherwise, that $W_C(X,Y) = W_C(Y,X)$.

(d) Deduce from **(c)** that for every $j = 0, \ldots, n$, the number of codewords of weight j in a self dual code C is equal to the number of codewords of weight $n - j$.

2. **(a)** What is meant by the weight of a vector $\underline{v} \in \mathbb{F}_q^n$? Define the term *minimum distance of a code*.

Vectors $\underline{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and $\underline{x}' = (x'_1, \ldots, x'_{n'}) \in \mathbb{F}_q^{n'}$ can be concatenated to form a vector $(\underline{x}, \underline{x}') = (x_1, \ldots, x_n, x'_1, \ldots, x'_{n'})$ in $\mathbb{F}_q^{n+n'}$.

Let $C \subseteq \mathbb{F}_q^n$ and $C' \subseteq \mathbb{F}_q^{n'}$ be non-zero codes of type $[n,k,d]$ and $[n',k',d']$ respectively. Form the code $C \oplus C'$ as the subspace of $\mathbb{F}_q^{n+n'}$ consisting of all the pairs $(\underline{v}, \underline{v}')$ where $\underline{v} \in C$ and $\underline{v}' \in C'$ (by this we mean "concatenation" of $\underline{v}$ and $\underline{v}'$. You are NOT required to show that $C \oplus C'$ is a subspace of $\mathbb{F}_q^{n+n'}$).

(b) Show that for every $\underline{x} \in \mathbb{F}_q^n$ and $\underline{x}' \in \mathbb{F}_q^{n'}$ one has $w((\underline{x}, \underline{x}')) = w(\underline{x}) + w(\underline{x}')$.

(c) Show that $C \oplus C'$ has dimension $k + k'$ and minimum distance $\min\{d, d'\}$.

(continued on next page)

(d) Show that $(\underline{x},\underline{x}')\bullet(\underline{y},\underline{y}')=\underline{x}\bullet\underline{y}+\underline{x}'\bullet\underline{y}'$ for any $\underline{x},\underline{y}\in\mathbb{F}_q^n$ and $\underline{x}',\underline{y}'\in\mathbb{F}_q^{n'}$.

Use this to prove that $C^\perp\oplus C'^\perp\subseteq(C\oplus C')^\perp$. Calculate the dimensions of these codes and deduce that in fact equality holds: $C^\perp\oplus C'^\perp=(C\oplus C')^\perp$.

3. **(a)** Explain the term *perfect code*.

(b) Let V denote $\mathbb{F}_2^m$ for some $m>1$. Recall that Hamming's code of length 2^m-1 is defined as the subspace C of $\Gamma(V-\{\underline{0}\};\mathbb{F}_2)$ consisting of the functions $f:V-\{\underline{0}\}\to\mathbb{F}_2$ which satisfy

$$\sum_{\underline{x}\in V-\{\underline{0}\}} f(\underline{x})\,\underline{x}=\underline{0}.$$

Show that C has parameters $[2^m-1,2^m-1-m,3]$.

(c) Show that given two distinct codewords $\underline{x},\underline{y}$ in a code C of type $[n,k,d]$ then the open balls $B(\underline{x},\frac{d}{2})$ and $B(\underline{y},\frac{d}{2})$ are disjoint. Use the fact that $\#B(\underline{x},\frac{d}{2})=\sum_{j=0}^{e}\binom{n}{j}(q-1)^j$ for any vector $\underline{x}$ to prove Hamming's bound

$$\sum_{j=0}^{e}\binom{n}{j}(q-1)^j\leq q^{n-k}.$$

(d) State Hamming's criterion for perfectness of codes and use it to show that the Hamming codes ($m>1$) are perfect.

4. **(a)** Explain what a *check matrix* of a code is.

(b) Fix a finite field $\mathbb{F}_q$ and $k\leq q$. Recall that the Reed-Solomon code $RS_k(q)$ over $\mathbb{F}_q$ is defined as the subspaces of polynomial functions of degree $<k$ in $\Gamma(\mathbb{F}_q,\mathbb{F}_q)$.

Prove that $RS_k(q)$ has parameters $[q,k,q-k+1]$ provided $k>0$.

(c) Recall that vectors $\underline{v}_1,\ldots,\underline{v}_k$ in a vector space V are called *linearly dependent* if there exist $\lambda_1\ldots,\lambda_k$ in $\mathbb{F}_q$, not all zero, such that $\sum_{i=1}^k\lambda_i\,\underline{v}_i=\underline{0}$.

Consider a code C of type $[n,k,d]$ where $k\geq1$ with a check matrix H. Use the fact that in $\mathbb{F}_q^m$ any $m+1$ vectors are linearly dependent, to deduce that C contains a non-zero vector $\underline{v}$ whose weight is $\leq n-k+1$.

(d) State Singleton's bound relating the minimal distance d of a code C with its dimension k and its length n. Deduce it from **(c)**, or otherwise.

Show that the Reed-Solomon codes attain this bound.