In the name of God

Finite Fields EXAM 25/01/2006

1. For any finite field K and a finite extension F of K, there exists a normal basis of F over K.

2. Let $f \in \mathbb{F}_q[x]$ be the polynomial of positive degree with $f(0) \neq 0$. Let r be the least positive integer for which x^r is congruent mod $f(x)$ to some element of $\mathbb{F}_q$, so that $x^r \equiv a \bmod f(x)$ with a uniquely determined $a \in \mathbb{F}_q^*$. Then $\operatorname{ord}(f) = hr$, where h is the order of a in the multiplicative group $\mathbb{F}_q^*$.

3. The monic polynomial is a q-polynomial over $\mathbb{F}_q$ if and only if each root of $L(x)$ has the same multiplicity, which is either 1 or a power of a q, and the root form a q-modulus (Prove both sides exactly).

4. Compute the minimal polynomials over $\mathbb{F}_3$ of all elements of $\mathbb{F}_9$.

5. Describe exactly the method of finding the roots of an affine q-polynomial $A(x) \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^m}$. Also describe the algorithm of finding the roots of an arbitrary polynomial $f(x) \in \mathbb{F}_q[x]$ over $\mathbb{F}_{q^m}$ using the notion of the affine multiple.

6. Determine the standard generator and the standard parity-check matrix of the binary linear $[5,3]$-code C defined by the generator matrix G. Find all codewords, the minimum distance and the weight enumerator of C. Also verify the MacWilliams Identity for C

$$G = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

In the name of God

Finite Fields

(Final Exam, June, 9, 2005)

1. Let $F = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$. Consider both F and K as vector spaces over K.
   (a) Show that $\mathrm{Tr}_{F/K} : F \longrightarrow K$ is a surjective linear transformation.

   (b) If $\beta \in F$ and $L_\beta : F \longrightarrow K$ is defined by $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$, show that $\mathrm{Hom}_K(F, K) = \{L_\beta \mid \beta \in F\}$, where $\mathrm{Hom}_K(F, K)$ is the set of linear transformation from F to K. Furthermore $L_\beta \neq L_\gamma$ whenever $\beta \neq \gamma$.

2. A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree m is a primitive polynomial over $\mathbb{F}_q$ if and only if f is monic, $f(0) \neq 0$, and $\mathrm{ord}(f) = q^m - 1$.

3. Let $f(x)$ be an irreducible polynomial in $\mathbb{F}_q[x]$ and let $F(x)$ be its linearized q-associate. Then the degree of every irreducible factor of $F(x)/x$ in $\mathbb{F}_q[x]$ is equal to $\mathrm{ord}(f)$.

4. (a) If $f(x) \in \mathbb{F}_q[x]$ is monic and $h(x) \in \mathbb{F}_q[x]$ is such that $h^q \equiv h \bmod f$, then
$$f(x) = \prod_{c \in \mathbb{F}_q} \gcd(f(x), h(x) - c).$$
   (b) Show that in view of the above equation and when q is small, we can find the canonical factorization of $f(x)$. Describe the Berlekamp factorization algorithm.
   (c) What can we do when q is large? Explain

5. Describe the following concepts: periodic sequence, ultimately periodic sequence, impulse response sequence, characteristic and minimal polynomial of a sequence, generating functions, (n, k)-linear code, parity check matrix, cyclic code.

6. Let $\theta \in \mathbb{F}_{64}$ be a root of the irreducible polynomial $x^6 + x + 1 \in \mathbb{F}_2[x]$. Find the minimal polynomial of $\beta = 1 + \theta^2 + \theta^3$ over $\mathbb{F}_2$.